U.S. Army War College
Dept. of Military Strategy, Planning, and Operations
&
Center for Strategic Leadership

November 2009
AY10 Edition

U.S. Army War College

Information Operations Primer

Fundamentals of Information Operations

Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE **NOV 2009**	2. REPORT TYPE	3. DATES COVERED **00-00-2009 to 00-00-2009**

4. TITLE AND SUBTITLE
Information Operations Primer

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
U.S. Army War College,Center for Strategic Leadership,650 Wright Avenue,Carlisle,PA,17013-5049

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**196**	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std Z39-18

Middle States Accreditation

The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

DEPARTMENT OF THE ARMY
UNITED STATES ARMY WAR COLLEGE AND CARLISLE BARRACKS
CARLISLE, PENNSYLVANIA 17013-5217

REPLY TO
ATTENTION OF

ATWC-A 15 November 2009

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: US Army War College Information Operations Primer

This is a document prepared primarily for use by the staff, faculty, and students of the U.S. Army War College. However, U.S. Government (USG) agencies and organizations may reprint this document, or portions of it, without further permission from the U.S. Army War College. Further, USG agencies and organizations may post this document wholly, or in part, to their official approved websites. Non-DoD individual or organization requests to reprint will be handled on a case-by-case basis.

William T. Johnsen
WILLIAM T. JOHNSEN, Ph.D.
Dean of Academics

DISTRIBUTION:
DMSPO 500

This Page Intentionally Blank

Foreword

This latest revision of the Information Operations Primer provides an overview of Department of Defense (DoD) Information Operations (IO) doctrine and organizations at the joint and individual service levels. It is primarily intended to serve students and staff of the US Army War College as a ready reference for IO information extracted and summarized from a variety of sources. Wherever possible, Internet web sites have been given to provide access to additional and more up-to-date information. The booklet is intentionally UNCLASSIFIED so that the material can be easily referenced during course work, while engaged in exercises, and later in subsequent assignments.

This booklet begins with an overview of Information Operations and Strategic Communication. (Note: as the emergent concept of Strategic Communication continues to assume increasing importance, the Primer has expanded to include discussion and input of this topic). Additionally, this year we have added an overview of cyberspace and cyberspace operations, which are now important emerging concepts. The booklet then goes from the national level to the Department of Defense, to the Combatant Command level and then finally to the service level. At each level it describes strategies or doctrine, agencies, organizations, and educational institutions dedicated to the information element of national power. Finally, the document concludes with an overview of Information Operations Condition (INFOCON) and an IO specific glossary.

Readers will note that many of the concepts, documents, and organizations are “works in progress” as DoD and the services strive to address the challenges of a rapidly changing IO environment. Thus, this summarization effort is on-going and continuous. Please address any suggested additions, revisions and/or corrections to the primary points of contact below for inclusion in subsequent editions.

Department of Military Strategy, Planning, and Operations
U.S. Army War College
122 Forbes Avenue
Carlisle Barracks, PA 17013-5242
717-245-3491
carl_ATWC-ASP@conus.army.mil

LTC John H. Greenmyer III
Department of Military Strategy,
Planning, and Operations
U. S. Army War College

Professor Dennis M. Murphy
Professor of Information Operations/Information
in Warfare
U.S. Army War College, Center for Strategic Leadership

This Page Intentionally Blank

Summary of Changes from the AY 09 Edition to the AY10 Edition of the IO Primer

The following changes have been made in this edition of the IO Primer:

Additions:

Essay on Cyberspace and Cyberspace Operations

Definition of Cyberspace Operations in the glossary

Description of 24th Air Force and subordinate units

Deletions:

Description of 8th Air Force

Description of Air Force Information Operations Center

Revisions:

The "Information Operations" and "Strategic Communication" sections have been updated.

All Department of Defense and Department of State agency sections have been updated where appropriate. Every section has been reviewed by the responsible office and most sections have some changes.

This Page Intentionally Blank

Acknowledgment of Thanks

A special thanks and recognition is given to the following individuals throughout the Department of Defense and Department of State whose help and assistance have made this revision of the Primer possible: LTC Maura A. Gillen from OSD-PA Joint Communication; Ambassador Brian E. Carlson from the Office of the Under Secretary of State for Public Diplomacy and Public Affairs; Mr. Brian Gouker from the National Security Agency; Mr. Andrew Lucas from the office of the Under Secretary Of Defense – Policy; Mr. David Chesterman from the office of the Under Secretary Of Defense for Intelligence; Ms. Patti Benner of the office of the Assistant Secretary Of Defense – Networks And Information Integration (ASD(NII)); Mr. Jon Anderson and Ms. Lillie Cofield of the Defense Information Systems Agency; Mr. Ryan Skousen, from the Information Assurance Technology Analysis Center; Mr. Roberto Rodriguez from the Joint Staff; Deputy Director for Global Operations; Ms. Elissa Bendell from the Joint Spectrum Center; CDR Curtis Plunk, USN, from the Joint Warfare Analysis Center; MAJ Bren Workman, USA, from the U.S. Strategic Command; Mr. Jerry R. Luss from the Joint Task Force – Global Network Operations; Mr. Larry McManus from the Joint Information Operations Warfare Center; Mr. Ken McGraw, from the U. S. Special Operations Command; LTC Cynthia Hazel, USA, from the Joint Military Information Support Command; Mr. Tony Billings from the Joint Public Affairs Support Element; COL Carmine Cicalese, USA, Chief Information Operations Division, Joint Command, Control, and Information Operations School, Joint Forces Staff College; Mr. Steve Iatrou from the Information Operations Center of Excellence, Naval Postgraduate School: Mr. Paul Palmer and COL Mike Dominique USA, both from the Army Combined Arms Center; Mr, Dave MacEslin, Doctrine Officer. IO Readiness Directorate Navy Information Operations Command Norfolk; Major Nichole Oliver, USAF, Chief ISR Branch, USAF LeMay Center/DDS; Mr. Rustin Vansickle and Mr. Matthew LaChance from the 1st Information Operations Command; LTC John W. Garnsey, DCDR, Army Reserve Information Operations Command; SSgt Jillian Pass and MSG Jonathan Wasilewski, USAF from the Air Force Intelligence, Surveillance and Reconnaissance Agency; Maj Richard Komurek, USAF, from the Eighth Air Force, Capt Carrie L. Kessler, 39 IOS PA Instructor, Hurlbert Field; Capt Eric R. Bixby, USAF, 24th Air Force and Mr. Jerry Johnson from the Center for Strategic Leadership, U.S. Army War College.

LTC John H. Greenmyer III
Department of Military Strategy,
Planning, and Operations
U. S. Army War College

Professor Dennis M. Murphy
Professor of Information Operations/Information
in Warfare
U.S. Army War College, Center for Strategic Leadership

This Page Intentionally Blank

TABLE OF CONTENTS

Information Operations

Notes on Changes: This introduction examines IO conceptually and doctrinally, but is intended only as a guide to facilitate academic discussion and is not authoritative. Both Army and Joint doctrine for Information Operations are being revised and will also likely be affected by the recent activation of U.S. Cyber Command. While the information in this is current as of publication, readers should consult the following sites for updates and changes:
http://www.dtic.mil/doctrine/jpoperationsseriespubs.htm (JP 3-13, Joint IO doctrine)
http://www.dtic.mil/doctrine/jpreferencepubs.htm (Joint dictionary)
http://www.army.mil/usapa/doctrine/Active_FM.html (FM 3-13, Army IO doctrine)

Background: Information Operations are an evolving construct with roots back to antiquity, thus it is both an old and a new concept. The late 1970's saw the emergence of Information Warfare (IW) and Command and Control Warfare (C2W) as war-fighting constructs integrating several diverse capabilities. These further evolved into Information Operations, recognizing the role of information as an element of power across the spectrum of peace, conflict, and war.

1. **IO is an Integrating Function.** Information Operations are the integration of capabilities involving information and information systems in order to gain a military advantage. This concept is similar to Joint Operations which are the integration of service capabilities or Combined Operations which are the integration of two or more forces or agencies of two or more allies. The integration envisioned is not mere deconfliction, but the synchronization of activities leading to action, and in turn, achieving desired effects that are significantly greater than the sum of the individual components. Several questions logically follow:

a. What is the purpose of IO?

b. What capabilities are integrated?

c. How are they integrated?

2. **Purpose of IO.** **Information Operations seek to influence the *behavior* of target decision-makers while simultaneously defending friendly decision-makers from being influenced by an adversary's use of information.** This is no different from the exercise of the other forms of national power. In this instance the means is information, but the resulting outcome is the same.

a. While frequently referred to as "soft-power" or "non-kinetic," IO includes the use of physical attack against adversary information systems or directly against decision makers. IO also employs technology-based activities to affect adversary information systems.

b. Affecting the target's decision cycle (sometimes referred to as his "OODA-loop" (observe, orient, decide, act - loop)) is a means of influencing target behavior. Obviously, reducing an adversary's ability to make timely and effective decisions will degrade his exercise of initiative or his response to friendly military action.

c. Action must also be taken to shield or protect friendly information and information systems from compromise or disruption. As a network-enabled force, the United States is particularly reliant on these systems to maintain situational awareness and to command and control forces. These protective actions are not intended to prevent the unrestricted flow of information vital to a free society, but rather to prevent a target's manipulation or distortion of information or attacks on information systems from being effective.

3. **An IO Conceptual Model.** At this point, a model would be helpful to conceptualize the kind of activities which would be effective in achieving the desired result (influence target behavior, protect friendly behavior from being influenced).

a. All Information Operations activities occur within the broader context of an ***information environment***. This environment recognizes the critical role that information and information systems play in today's advanced societies as they progressed along a continuum from agrarian, to industrial, to the information age. This environment pervades and transcends the boundaries of land, sea, air, space, and cyberspace. It is accessible and leveraged by both state and non-state actors.

b. Within this environment exist three conceptual dimensions: physical, information, and cognitive as depicted in Figure 1, representing a target's decision cycle.

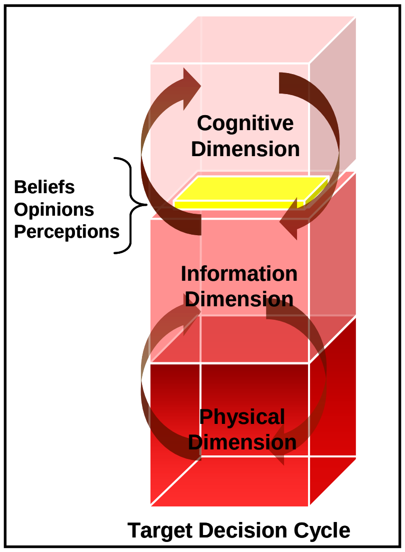


Figure 1. The Information Environment

(1) The physical dimension is the tangible real world. It is the dimension where military operations take place within the land, sea, air, space, and cyberspace environments. Information and communications systems exist within this dimension to enable these operations to take place.

(2) The information dimension is where information is created, manipulated, shared, and stored. This dimension links the physical real world with the human consciousness of the cognitive dimension both as a source of input (stimulus, senses, etc.) and to convey output (intent, direction, decisions, etc.). These linkages are shown as arrows in the figure.

(3) The cognitive dimension exists in the mind. This is where the individual processes the received information according to a unique set of perceptions (interprets the information), opinions (within a greater context of how he sees the world organized), and beliefs (on a foundation of core central values). These attributes act as a "window" to filter the information and provide a sense of meaning and context. The information is evaluated and processed (via an OODA loop or other model) to form decisions which are communicated back through the information dimension to the physical world. It should be noted that the cognitive dimension cannot be directly attacked (short of mind-altering drugs) but must be influenced indirectly through the physical and information dimensions.

(4) Not shown in the figure is an additional "social" dimension which links the individual to others, forming a greater social network. This social network plays a critical role in the human decision-making process as well.

c. In a similar manner, the friendly decision cycle can be represented in relationship to the target as shown in Figure 2. This allows several terms to be defined conceptually.

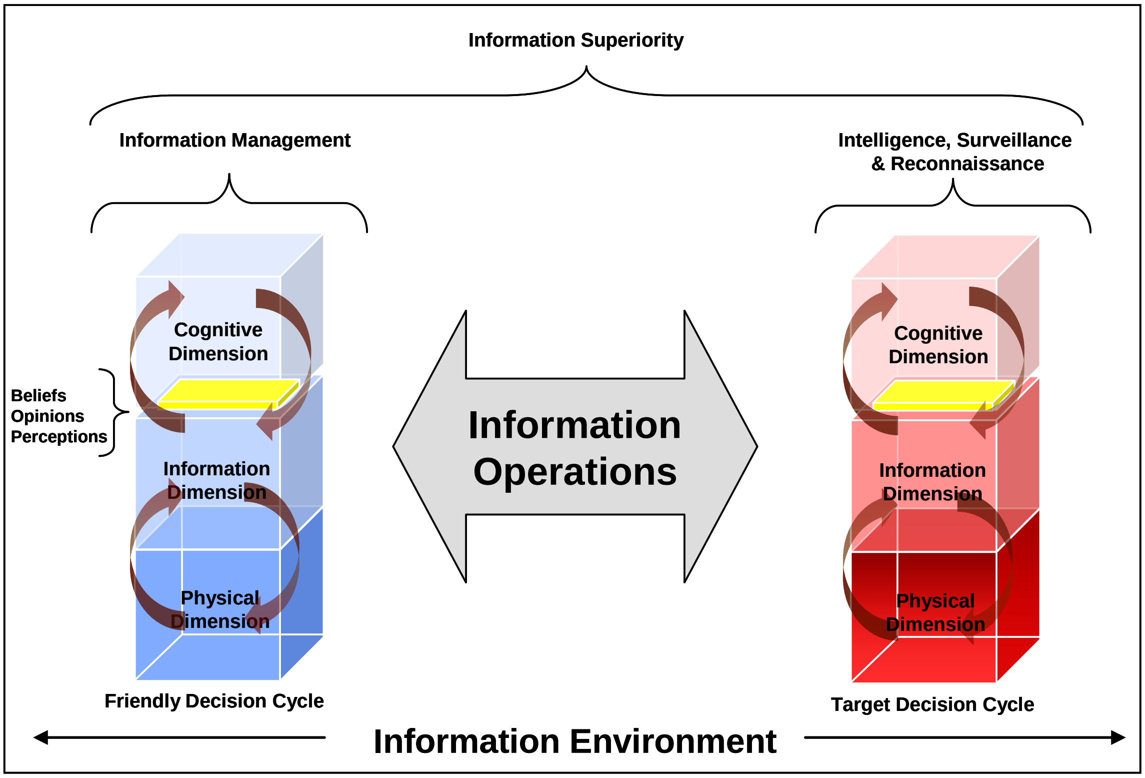


Figure 2. A Notional Information Operations Model

(1) **Intelligence, Surveillance, and Reconnaissance (ISR)** are those activities which synchronize and integrate the planning and operation of sensors, assets, processing, exploitation, and dissemination systems to gain information and knowledge concerning a target (adversary). The focus is strictly on target information and information systems.

(2) Correspondingly, **Information Management (IM)** and **Information Assurance (IA)** activities seek to provide the right information to the right individual at the right time in a usable form to facilitate situational understanding and decision-making. The focus is on friendly information and information systems, their protection, accuracy and timeliness.

(3) The third type of activity relates to both friendly and target decision cycles. These activities are **Information Operations (IO)** as indicated in Figure 2. IO in this figure represents the offensive engagement in the information domain.

(4) Considering these three sets of activities as a whole yields **Information Superiority** which, when achieved, results in a degree of dominance in the information domain (environment) permitting the conduct of operations without effective opposition. Information Superiority is a key enabler of strategic war fighters.

d. Information Operations can now be depicted as attempting to influence, disrupt, corrupt, or usurp adversarial human or automated decision-making while protecting friendly decision-making as shown in Figure 3.

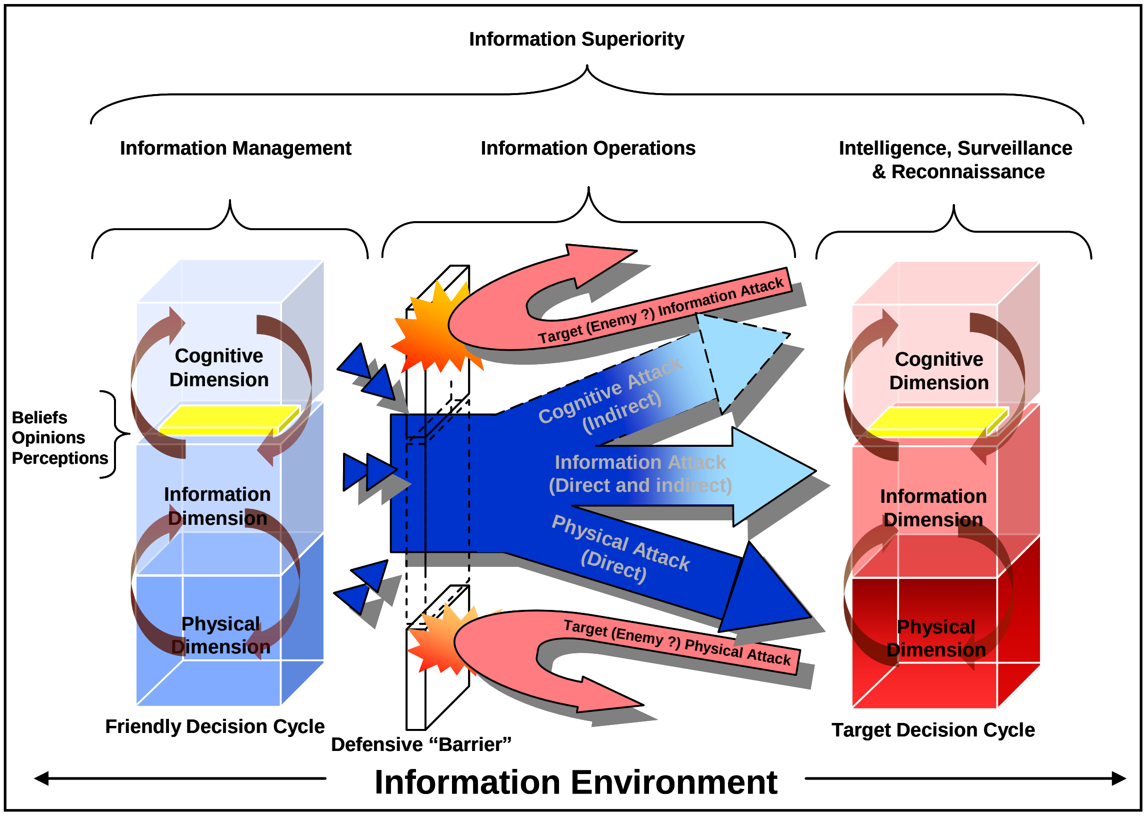


Figure 3. Information Operations Conceptual Framework

4. <u>IO Capabilities.</u> Using this framework, it is now possible to address the question of what capabilities are integrated by IO. These capabilities will be further categorized as either core, supporting, or related.

a. ***Core Capabilities*** are those which are essential to the conduct of IO by providing critical operational effects or preventing the adversary from doing so. The five core capabilities of Psychological Operations (PSYOP), Military Deception (MILDEC), Operations Security (OPSEC), Electronic Warfare (EW), and Computer Network Operations (CNO) form the foundation for IO.

(1) **Psychological Operations (PSYOP)** are planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals. The purpose of psychological operations is to induce or reinforce foreign attitudes and behavior favorable to the originator's objectives.

(2) **Military Deception (MILDEC)** consists of actions executed to deliberately mislead adversary military decision makers as to friendly military capabilities, intentions, and operations, thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly mission.

(3) **Operations Security (OPSEC)** is a process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to:

(a) identify those actions that can be observed by adversary intelligence systems;

(b) determine indicators that adversary intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries; and

(c) select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation.

(4) **Electronic Warfare (EW)** is any military action involving the use of electromagnetic and directed energy to dominate the electromagnetic spectrum or to attack the enemy. The three major subdivisions within electronic warfare are as follows:

(a) Electronic Attack (EA)**.** That division of electronic warfare involving the use of electromagnetic energy, directed energy, or anti-radiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability and is considered a form of fires. EA includes: 1) actions taken to prevent or reduce an enemy's effective use of the electromagnetic spectrum, such as jamming and electromagnetic deception, and 2) employment of weapons that use either electromagnetic or directed energy as their primary destructive mechanism (lasers, radio frequency weapons, particle beams).

(b) Electronic Protection (EP)**.** That division of electronic warfare involving passive and active means taken to protect personnel, facilities, and equipment from any effects of friendly or enemy employment of electronic warfare that degrade, neutralize, or destroy friendly combat capability.

(c) Electronic Warfare Support (ES). That division of electronic warfare involving actions tasked by, or under direct control of, an operational commander to search for, intercept, identify, and locate or localize sources of intentional and unintentional radiated electromagnetic energy for the purpose of immediate threat recognition, targeting, planning and conduct of future operations. Thus, electronic warfare support provides information required for decisions involving electronic warfare operations and other tactical actions such as threat avoidance, targeting, and homing. Electronic warfare support data can be used to produce signals intelligence, provide targeting for electronic or destructive attack, and produce measurement and signature intelligence.

(5) **Computer Network Operations (CNO).** Comprised of computer network attack, computer network defense, and related computer network exploitation enabling operations.

(a) Computer Network Attack (CNA). Actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves.

(b) Computer Network Defense (CND). Actions taken through the use of computer networks to protect, monitor, analyze, detect and respond to unauthorized activity within Department of Defense information systems and computer networks.

(c) Computer Network Exploitation (CNE). Enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks.

b. These five core capabilities are supported by five additional, or ***Supporting Capabilities*** which provide additional operational effects: Information Assurance (IA), Physical Security, Physical Attack, Counterintelligence (CI), and Combat Camera (COMCAM).

(1) **Information Assurance (IA)** is defined as measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

(2) **Physical Security** is that part of security concerned with physical measures designed to safeguard personnel; to prevent unauthorized access to equipment, installations, material, and documents; and to safeguard them against espionage, sabotage, damage, and theft. The physical security process includes determining vulnerabilities to known threats, applying appropriate deterrent, control, and denial safeguard techniques and measures, and responding to changing conditions.

(3) **Physical Attack** disrupts, damages, or destroys adversary targets through destructive power. Physical attack can also be used to create or alter adversary perceptions or drive an adversary to use certain exploitable information systems.

(4) **Counterintelligence (CI)** consists of the information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassination conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities.

(5) **Combat Camera (COMCAM)** consists of the acquisition and utilization of still and motion imagery in support of combat, information, humanitarian, special force, intelligence, reconnaissance, engineering, legal, public affairs, and other operations involving the Military Services.

c. Finally, three additional ***Related Capabilities*** of Public Affairs (PA), Civil-Military Operations (CMO), and Defense Support to Public Diplomacy (DSPD) contribute to the accomplishment of the IO mission. These activities often have regulatory, statutory, or policy restrictions and limitations regarding their employment which must be observed.

(1) **Public Affairs (PA)** are those public information, command information, and community relations activities directed towards both the external and internal publics with interest in the Department of Defense.

(2) **Civil-Military Operations (CMO)** are the activities of a commander that establish, maintain, influence, or exploit relations between military forces, governmental and nongovernmental civilian organizations and authorities, and the civilian populace in a friendly, neutral, or hostile operational area in order to facilitate military operations, to consolidate and achieve operational US objectives. Civil-military operations may include performance by military forces of activities and functions normally the responsibility of the local, regional, or national government. These activities may occur prior to, during, or subsequent to other military actions. They may also occur, if directed, in the absence of other military operations. Civil-military operations may be performed by designated civil affairs, by other military forces, or by a combination of civil affairs and other forces.

(3) **Defense Support to Public Diplomacy (DSPD)** are those activities and measures taken by the Department of Defense components to support and facilitate public diplomacy efforts of the United States Government (previously referred to as Military Support to Public Diplomacy).

d. These capabilities can be summarized as shown in the following table.

CORE CAPABILITIES	
Electronic Warfare Computer Network Operations Operations Security	Military Deception Psychological Operations
SUPPORTING CAPABILITIES	**RELATED CAPABILITIES**
Information Assurance Physical Security Counterintelligence Physical Attack Combat Camera	Public Affairs Civil-Military Operations Defense Support to Public Diplomacy

DoD Information Operations: "The integrated employment of the core capabilities of electronic warfare, computer network operations, psychological operations, military deception, and operations security, in concert with specified supporting and related capabilities, to influence, disrupt, corrupt or usurp adversarial human and automated decision-making, while protecting our own."

Table 1. Joint IO Capabilities and Definition

e. These activities can be related to the IO Conceptual Framework previously described in terms of offensive and defensive actions as well as in terms of their orientation with respect to the cognitive, information, and physical dimensions. An additional distinction which may be helpful is to further categorize the activities into those which are primarily "influential" in nature (MILDEC, PSYOP, PA, etc.) and those which are more "technical (or electronic)" in nature (EW and CNO, etc.).

5. **IO Planning and Execution.** Having identified the purpose of IO and the activities associated with it, the third question will now be addressed concerning how IO capabilities are integrated.

a. Information Operations are planned by the IO section of a joint or service staff under the direction and supervision of a designated IO officer. Within a joint command, such as a Combatant Command, this section normally resides within the operations directorate (J-3) of the staff, often designated the J-39. Representatives from the core, supporting, and related capabilities as well as the special staff, service/functional components, and appropriate national agencies serve as members of the J-39.

b. IO planning must be fully integrated into the overall joint planning process, be it contingency or crisis action. There should not be a separate "IO campaign plan" just as there is no separate "maneuver campaign plan." Additionally, visualizing "information" as a separate Line of Operation (LOO) does improve visibility of IO, but it is at the cost of obscuring how (or whether) IO has properly coordinated support to the other LOOs. Commanders who describe and visualize IO as something separate will likely find that it becomes something separate.

c. Products from the IO planning process are incorporated into the Commander's Estimate, Commander's Concept, and the OPLAN/OPORD as documented in the Joint Operation Planning and Execution System (JOPES).

d. Evaluation of the success of the execution of the plan is done through identified measures of effectiveness (MOE), which is how well the plan achieved the desired result, and measures of performance, which is how well the plan was executed. MOE and MOP must be identified as a component of the IO planning process based upon realistic expectations for timeliness and accuracy of data received.

6. **Additional Considerations.**

a. While not yet captured in doctrine as an IO capability, personal interactions are perhaps the most important means a target audience can be influenced. In the context of persuasive influence, these interactions can range from compulsion and coercion on one end of the spectrum to cooperation and collaboration on the other. Viewed in the terms of the amount of planning involved, they can vary from deliberate meetings between a carefully chosen messenger and an influential target covering specific issues, or chance meetings between "Joe" and random members of the populace.

b. Regardless of how the message is transmitted, the credibility of our messages and messengers is key to the effectiveness of our influence efforts. We must recognize that we lose credibility when the implied messages of our actions do not match the messages of our overt communications. If these messages are not coordinated during the IO planning process, our credibility and effectiveness suffer.

c. An appropriate understanding of the target's culture and norms is essential to effective information operations. Our communications efforts must avoid the tendency to "mirror" friendly cultural values and perspectives, but rather must be prepared, executed and evaluated from the perspective of the target audience, through their cultural lens.

d. Even when done effectively, IO effects typically take longer to achieve and are more difficult to measure than conventional operations. Therefore, a long term commitment to building relationships and maintaining communication (two-way dialog) is critical. Theater Security Cooperation Plans are a vital part of this effort. Waiting until a crisis occurs and then "throwing info ops at it" is an exercise in futility.

Effective IO leverages the power of information to complement the other instruments of national power resulting in the achievement of national objectives with less expenditure of blood and treasure.

This original essay was written by Professor David Smith, now with the Information in Warfare Group, CSL, USAWC and was reviewed and updated by LTC John Greenmyer.

LTC John H. Greenmyer III
Department of Military Strategy,
Planning, and Operations
U.S. Army War College

Updated: October 2009

Strategic Communication

Strategic Communication. This section addresses some considerations of the information element of power at the strategic level.

a. Information and National Power. Interestingly, one needs to go back to the Reagan administration to find the most succinct and pointed mention of information as an element of power in formal government documents.[1] Subsequent national security documents allude to different aspects of information but without a specific strategy or definition. Still, it is generally accepted in the United States government today that information is an element of national power along with diplomatic, military and economic power…and that information is woven through the other elements since their activities will have an informational impact.[2] Given this dearth of official documentation, Drs. Dan Kuehl and Bob Nielson proffered the following definition of the information element: "use of information content and technology as strategic instruments to shape fundamental political, economic, military and cultural forces on a long-term basis to affect the global behavior of governments, supra-governmental organizations, and societies to support national security."[3] Information as power is wielded in an increasingly complex environment consisting of the physical, information, and cognitive dimensions as previously defined.

b. Strategic Communication Overview. The executive branch of the US government has the responsibility to develop and sustain an information strategy that ensures strategic communication occurs consistent with and in support of policy development and implementation. This strategy should guide and direct information activities across the geo-strategic environment**.** Effective strategic communication is the desired "way" (given the "ends, ways, means" model) that information is wielded in accordance with that strategy. It is formally defined as "focused United States Government processes and efforts to understand and engage key audiences in order to create, strengthen, or preserve conditions favorable to advance national interests and objectives through the use of coordinated information, themes, plans, programs, and actions synchronized with other elements of national power." Parsing this rather bureaucratic definition to its essentials, strategic communication is the orchestration of actions, words and images to achieve cognitive effects in support of policy and military objectives. While the capabilities used to achieve those effects should be unconstrained, primary supporting capabilities of strategic communication at the national strategic level are generally considered as Public Affairs (PA); military Information Operations (IO) and Public Diplomacy (PD).[4]

(1) Public affairs and military IO have been defined in the context of their use within the Department of Defense (DOD) in the previous section.

(2) Public diplomacy is primarily practiced by the Department of State (DOS). It is defined as "those overt international public information activities of the United States Government designed to promote United States foreign policy objectives by seeking to understand, inform, and influence foreign audiences and opinion makers, and by broadening the dialogue between American citizens and institutions and their counterparts abroad."[5]

(3) International broadcasting services are cited as a strategic communication means in some definitions. Under the supervision of the Broadcasting Board of Governors (BBG), the International Broadcasting Bureau (IBB) provides the administrative and engineering support for U.S. government-funded non-military international broadcast services. Broadcast elements are the Voice of America (VOA) and Radio and TV Martí (Office of Cuba Broadcasting). In addition, the IBB provides engineering and program support to Radio Free Europe/Radio Liberty, Radio Free Asia, and the Middle East Broadcasting Networks (Radio Sawa and Alhurra Television).[6]

Strategic communication is considered by some to be solely a national strategic concept, however, it is increasingly recognized as occurring at all levels from tactical to strategic, despite the lexicon of the term itself.

c. History of Strategic Communication. While "strategic communication" is a fairly new term in the U.S. government parlance, the concept, theory, and practice behind it is not. Winfield Scott recognized the importance of strategic communication at the theater level in Veracruz in 1847. Realizing the influence of the Catholic Church on Mexican society, Scott attended Mass with his staff at the Veracruz Cathedral to display the respect of U.S. forces. He further ordered U.S. soldiers to salute Mexican priests in the streets. Each of these measures was "part of a calculated campaign to win the friendship of the Mexicans."[7]

The recent history of national strategic communication shows concerted efforts to positively portray the U.S. story in order to persuade and influence.

(1) The Committee on Public Information (1917), also known as the Creel Committee after its chief, newspaperman George Creel, sought to rally U.S. public opinion behind World War I on behalf of the Wilson administration. Its focus was the domestic audience and it used public speakers, advertising, pamphlets, periodicals, and the burgeoning American motion picture industry.

(2) The Office of War Information (1942) focused both domestically and overseas, with broadcasts sent in German to Nazi Germany. The Voice of America (VOA) began its first broadcast with the statement, "Here speaks a voice from America. Everyday at this time we will bring you the news of the war. The news may be good. The news may be bad. We shall tell you the truth."

(3) The Smith-Mundt Act (1948) (actually, "The U.S. Information and Educational Exchange Act (Public Law 402; 80th Congress)"), established a statutory information agency for the first time in a period of peace with a mission to "promote a better understanding of the United States in other countries, and to increase mutual understanding" between Americans and foreigners. The act also forbade the Voice of America to transmit to an American audience. It is worth noting that Smith-Mundt is often cited today as the basis to limit the use of government information activities to influence since it may result in "propagandizing" the American public. This, of course, is complicated by the inevitable "blowback" or "bleedover" of foreign influence activities based on the global information environment.[8]

(4) The United States Information Agency (USIA) (1953) was established by President Eisenhower as authorized by the Smith-Mundt Act. It encompassed all the information programs, including VOA (its largest element), that were previously in the Department of State, except for the educational exchange programs, which remained at State. The USIA Director reported to the President through the National Security Council and received complete, day-to-day guidance on U.S. foreign policy from the Secretary of State.

(5) A 1998 State Department reorganization occurred in response to calls by some to reduce the size of the U.S. foreign affairs establishment. (This is considered the State Department's "peace dividend" following the Cold War). The act folded the USIA into the Department of State. It pulled the Broadcasting Board of Governors out of USIA and made it a separate organization. The USIA slots were distributed throughout the State Department and its mission was given to the Bureau of International Information Programs.

d. National Strategic Communication: Current Models and Processes. The demise of USIA is generally regarded (in retrospect) as diluting the ability of the United States to effectively promulgate a national communication strategy, coordinate and integrate strategic themes and messages, and support public diplomacy efforts worldwide.[9] Additionally, organizations and processes have experienced great flux in recent years. Strategic communication efforts under the George W. Bush administration provided mixed results. While some interagency committees and offices were ineffective or became dormant, there was some notable progress under Ambassador Karen Hughes (who assumed duties as the Under Secretary of State for Public Diplomacy and Public Affairs in the early fall of 2005 and departed in late 2007). The Under Secretary helps ensure that public diplomacy (described as engaging, informing, and influencing key international audiences) is practiced in harmony with public affairs (outreach to Americans) and traditional diplomacy to advance U.S. interests and security and to provide the moral basis for U.S. leadership in the world.[10] Ambassador Hughes provided specific guidance to public affairs officers at embassies throughout the world that either shortcut or eliminated bureaucratic clearances to speak to the international press. She established a rapid response unit within the State Department to monitor and respond to world and domestic events. She reinvigorated the Strategic Communication Policy Coordinating Committee and established communication plans for key pilot countries. And she established processes to disseminate coordinated U.S. themes and messages laterally and horizontally within the government. Finally and perhaps most importantly, a long awaited National Strategy for Public Diplomacy and Strategic Communication was published under her leadership in May 2007.

The Obama administration's efforts to advance strategic communication efforts are nascent as of this writing. Judith McHale was sworn in as Undersecretary of State for Public Diplomacy and Public Affairs on May 26, 2009. A Global Engagement and Strategic Communication Interagency Policy Committee, which acts as a coordinating mechanism, is active and led by the National Security Council. Ms. McHale has retained many of Hughes' initiatives to include an interagency operational level Global Strategic Engagement Center which monitors, responds to and proactively considers global information messaging. It is unclear whether the national strategy developed under the previous administration will be officially recognized or modified by the Obama administration.

Additionally, an Interagency Strategic Communication Fusion Network remains an active, albeit informal, coordinating body at the action officer level. Network members share information about their respective plans and activities in order to leverage each other's communication with international publics. The network coordinates and de-conflicts the production and the dissemination of information products but does not task. Instead, network members reach across office, bureau and agency boundaries to offer or to seek support for their strategic communication plans and activities.[11]

The Defense Department has responded to the challenges posed by the current information environment, but also with mixed results. The 2006 Quadrennial Defense Review (QDR) conducted a spin off study on strategic communication that resulted in a roadmap addressing planning, resources and coordination. Perhaps the most important aspect of the roadmap is the stated objective of developing strategic communication plans in conjunction with policy development, thus fulfilling Edward R. Murrow's desire to be brought in on the takeoff, not the crash landing.[12] However, actions to achieve roadmap milestones are no longer formally monitored. On the other hand enduring "Principles of Strategic Communication" were published by the office of the Assistant Secretary of Defense (Public Affairs) in 2008 and are still accepted.[13]

e. Theater Strategic Communication. Theater strategic communication is an emergent concept with only brief discussion in Joint Publication 3-13 (Information Operations). However, because of the importance of the information element of power in the current military campaigns in Iraq and Afghanistan, combatant commanders have established processes and organizations to address the need. Various organizational models exist among the combatant commands from separate strategic communication directorates to incorporation of strategic communication processes into effects cells. As of September, 2008 it appeared that an organization consisting of a strategic communication director with small coordination staff and supporting strategic communication working group was becoming the norm.[14]

While national strategic communication lists principal capabilities of PA, PD and IO, DOD strategic communication (and thus combatant command strategic communication) includes military PA, defense support to public diplomacy (alternately referred to as military support to public diplomacy), aspects of IO (principally PSYOP), Military Diplomacy (MD) and Visual Information (VI).[15] The concept of defense support to public diplomacy is still vaguely defined with examples ranging from theater web initiatives aimed at certain regions and demographics within those regions to theater logistical support to embassies and diplomatic staffs. Military Diplomacy includes traditional interactions between U.S. senior military leaders and foreign military leaders. Beyond the importance of theater strategic communication in ongoing military operations, doctrine is correct to point out the importance of strategic communication activities in implementing theater security cooperation plans (TSCPs) based on its inherent shaping and deterrence capability.[16]

f. Ends, Ways, Means: Where Does Strategic Communication Fit? Strategists use a model of "ends, ways and means" to describe all aspects of a national or military strategy. Strategy is about how (the way) leaders will use the capabilities (means) available to achieve objectives (ends).[17] Understanding and engaging key audiences is meant to change perceptions, attitudes and, ultimately behaviors to help achieve military (and in turn national) objectives. Thus, parsing the QDR definition it is apparent that strategic communication is a "way" to achieve an information effect on the cognitive dimension of the information environment (the required "end"). Military leaders should not limit strategic communication means to only those primary capabilities listed in the definition. Strategic communication means should be restricted only by the requirement to achieve the desired information effect on the target audience.

In that light, messages are certainly sent by verbal and visual communications means, but they are also sent by actions. (Note that the QDR definition specifically includes "actions"). In fact, senior officials point out that strategic communication is "80% actions and 20% words."[18] Specifically, how military operations are conducted affects the information environment by impacting perceptions, attitudes and beliefs. As previously noted, DOD has emphasized this fact by referring to strategic communication as the orchestration of actions, images and words.

g. Strategic Communication and IO: A Side by Side Comparison. The current definitions of IO (Joint Publication 3-13) and Strategic Communication (QDR Strategic Communication Roadmap) are clear and fairly distinct to the fully engaged information practitioner, but there are nuances that make those distinctions difficult to grasp for others (to include operational commanders) and so clarifying these concepts is well worth considering. Strategic communication is the more broadly overarching concept targeting *key audiences* and focusing on the cognitive dimension of the information environment. IO as an integrating function, on the other hand, more specifically targets an *adversary's decision making capability* which may be in the cognitive, informational and/or physical dimensions of the information environment.

	Target	**Effect**	**Dimension**	**Primary Capabilities**
SC	Key audiences (friendly, neutral, adversarial)	Understand and engage	Cognitive (people)	PA, PSYOP, MD, DSPD, VI "actions, images, words"
IO	Adversarial human and automated decision-making	Influence, disrupt, corrupt, or usurp	Cognitive, information, physical (people, processes, systems)	EW, CNO, OPSEC, MILDEC, PSYOP

Considering the targets and effects described above, it should be clear that both strategic communication and IO can be employed at all levels of warfare (tactical, operational, theater strategic and national strategic). Tactical commanders routinely employ strategic communication in Iraq and Afghanistan today based on their interactions with key audiences in their area of responsibility to a potential strategic end.

On the other end of the scale, IO could certainly be employed strategically as part of a shaping Phase 0 operation or a deterrent Phase 1 operation against a potential adversary's decision-making capability.

h. Effectively Integrating Strategic Communication in Military Planning. Remembering that strategic communication is a way to achieve cognitive information effects using any means available takes the mystery out of the concept. Strategic communication simply employs capabilities (limited only to the imagination) to support the achievement of a military objective. Just as a commander integrates air, land and sea capabilities into military planning and execution, he can and should integrate strategic communication capabilities. The planning process is not new. The focus on and understanding of this new concept and its capabilities, however, may be.

First, planners must define the information environment and its physical, informational and cognitive dimensions. How does the target audience receive their information (TV, radio, internet, rumor, religious services, etc.)? How does culture play into the message? Who are the credible messengers? Next, planners need to consider the desired effect on the cognitive dimension, i.e. the ends or outcome. Does the endstate include changing perceptions, influencing people, gaining acceptance, gaining credibility and trust, gaining support? This will drive how the operation will be conducted where themes and messages are necessary, but not sufficient.

Any military planner will quickly see how this logical thought process fits neatly into the established military decision-making process (or campaign planning process). The information environment is considered in the analysis of the overarching operational environment. The commander's intent establishes an endstate. This must include a statement of the desired information environment endstate. A properly stated information endstate in the commander's intent will guide staffs in the selection of appropriate courses of action and drive subordinate units in the way they conduct operations to achieve that endstate. A selected course of action will then be wargamed using the traditional friendly action, expected enemy reaction, and friendly counteraction methodology. The wargaming process must also occur with an eye toward information effects. This becomes especially important in counterinsurgency operations where the enemy uses information as an asymmetric strategic means and where changing indigenous populations' perceptions can turn them from a neutral position to one in favor of coalition forces. But it also applies across all levels of the spectrum of conflict in an environment where military operations will likely be covered in real time by both mainstream and "new" media sources.

i. Conclusion. Strategic communication is simply a way to affect perceptions, attitudes and behaviors of key audiences in support of objectives. Certainly communications means are very important in ultimately achieving those desired information effects. But *how* military operations are conducted or policy is implemented is also a key component of strategic communication, since actions send very loud and clear messages. Effective strategic communication requires an organizational culture attuned to the information environment and a recognition that strategic communication, as a way to achieve information effects, consists of many capabilities (means) that are an integral part of the leader's arsenal.

This essay was written by Dennis M. Murphy, Professor of Information Operations / Information in Warfare, CSL, USAWC

Updated: October 2009

[1] Ronald Reagan, *National Security Decision Directive 130* (Washington, D.C.: The White House, 6 March 1984) Available from http://www.fas.org/irp/offdocs/nsdd/nsdd-130.htm. Internet. Accessed 01 October 2009.

[2] Emergent NATO doctrine on Information Operations cites Diplomatic, Military and Economic activities as "Instruments of Power." It further states that Information, while not an instrument of power, forms a foundation as all activity has an informational backdrop.

[3] Robert E. Neilson and Daniel T. Kuehl, "Evolutionary Change in Revolutionary Times: A Case for a New National Security Education Program," *National Security Strategy Quarterly* (Autumn 1999): 40.

[4] Various definitions of strategic communication exist with no overarching U.S. government definition. As of this writing, DOD is still debating the definition. The one shown here is taken from Department of Defense, QDR Execution Roadmap for Strategic Communication, (Washington, DC: U.S. Department of Defense, 25 September 2006), 3.

[5] U.S. Department of Defense, *DOD Dictionary*, http://www.dtic.mil/doctrine/jel/doddict/data/p/11548.html (accessed 01 October 2009).

[6] *Broadcasting Board of Governors Home Page*, http://www.bbg.gov/, (accessed 01 October 2009).

[7] John S.D. Eisenhower, *Agent of Destiny: The Life and Times of General Winfield Scott* (New York: The Free Press, 1997) 245-6.

[8] The Smith-Mundt Act is still in effect to include the requirement not to "target" U.S. audiences. The current information environment with ubiquitous, world-wide media outlets, satellite communications and real-time reporting makes it difficult to target foreign audiences without exposing U.S. audiences to the message, however…a fact not envisioned in 1948 when the act became effective and one that continues to cause friction between the military and media.

[9] David E. Kaplan "Hearts, Minds, and Dollars." *U.S. News and World Report*, April 25, 2005, 25, 27.

[10] "Senior Officials: Under Secretary for Public Diplomacy and Public Affairs -- Karen Hughes", linked from *U.S. Department of State Homepage* http://www.state.gov/misc/19232.htm (accessed 01 October 2009).

[11] Interagency Strategic Communication Fusion Network Agenda, 30 September 2009, 3.

[12] QDR Execution Roadmap for Strategic Communication, 3.

[13] U.S. Principal Deputy Assistant Secretary of Defense for Public Affairs Robert T. Hastings, "Principles of Strategic Communication," memorandum for Secretaries of the Military Departments, et. al., Washington, DC, August 15, 2008.

[14] U.S. Joint Forces Command, *Commander's Handbook for Strategic Communication* (Norfolk, VA: Joint Warfighting Center, September 1, 2008), III-7. This manual indicates that "eight combatant commands are either employing or transitioning to this model."

[15] QDR Execution Roadmap for Strategic Communication, 2.

[16] Chairman of the Joint Chiefs of Staff, *Information Operations*, Joint Publication 3-13, (Washington, DC: Joint Chiefs of Staff, February 13, 2006), I-13.

[17] Harry R. Yarger, "Toward a Theory of Strategy: Art Lykke and the Army War College Strategy Model," *U.S. Army War College Guide to National Strategy and Policy* (June 2006): 107.

[18] The author has attended numerous briefings by the Deputy Assistant Secretary of Defense for Joint Communication (DASD (JC)) and his staff where this has been stated. Note: the DASD (JC) is responsible for the DOD Strategic Communication Roadmap.

This Page Intentionally Blank

Cyberspace & Cyberspace Operations

This section addresses the evolving nature of cyberspace, specifically focusing on its influence on, and implications for, all instruments of national power. It also addresses the need for continued development of theory, organization, and mission for cyberspace operations related to national security.

1. Introduction.

a. Definition. DoD currently defines cyberspace as "a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers,"[1] and it can be argued this should also include their operators. In a broader sense, cyberspace is "a new strategic common, analogous to the sea as an international domain of trade and communication."[2]

b. History--Enduring vice Modern Cyberspace. In its simplest form, the cyberspace process consists of elements within the three dimensions of the overall information environment – cognitive, information, and physical.[3] For example, someone generates and articulates a thought (cognitive); they enter the thought into a communication device (physical) where it becomes a systematic representation of data (information), possibly represented digitally using electromagnetic means. Next, the data travels through a variety of physical lines of communication (e.g., telephone, cable, fiber optic, radio, microwave, etc) where it exits through a communication device to another user for cognitive uses, or perhaps to a physical device to perform an operation (e.g., turn on a light, open a valve, etc).

What is cyberspace, then? It is the total of all elements required for cyberspace processes to occur. The fundamental structure of the cyberspace process is enduring; but the configuration of cyberspace itself transforms when specific elements of the basic process transform. As depicted in Figure 1, the development of the telegraph is an early example of the cyberspace process evolution. In the mid-twentieth century, the process was transformed with the introduction of electronic transistor-based data processing devices. As currently envisioned, modern cyberspace came into existence due to the convergence of three events--the introduction of the personal computer (circa 1975), the Internet (circa 1982), and the worldwide web protocol (circa 1989). [4]

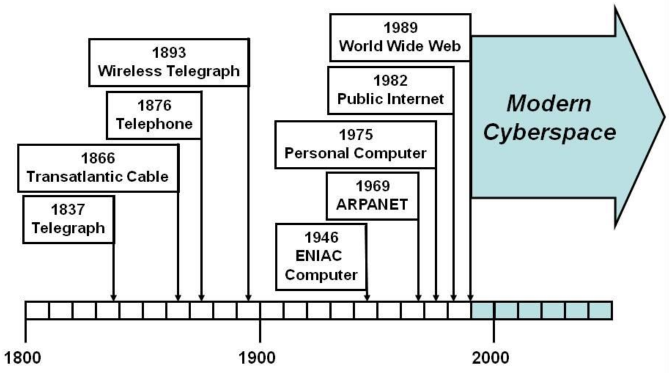


Figure 1. A Brief Timeline of Cyberspace Development

c. Cyberspace as a Global Common. The synergy of the events that established modern cyberspace also represents the creation of a new "strategic common" analogous to Mahan's theories where the sea is described as "a wide common" that is the international domain of commerce and communication.[5] Given such similar elements among the strategic commons, also called global commons, cyberspace has at least five unique characteristics of concern to strategic security leaders. First, the cost of entry and routine access to cyberspace is extremely low—basically the cost of a laptop and Internet café fee. Second, cyberspace offers a degree of anonymity that greatly challenges efforts to detect, track, and target a specific user who desires to hide in the common. Third, cyberspace provides the ability to initiate a wide variety of physical effects across vast distances at almost instantaneous speeds. Fourth, cyberspace itself is an ever-growing common; every new computer server or Internet-capable cell phone expands its boundaries. Also, cyberspace is mostly owned and operated by private parties (individuals and corporations). Finally, cyberspace does not have traditional dimensions of height, depth, and length, but it does have unique metrics that can be used to map its boundaries and operations.

2. Dynamic Nature of Contemporary Cyberspace Evolution.

a. Connectivity. Innovations in computer technology have greatly enhanced the ability of the average citizen to operate freely in cyberspace. Data processing speeds and digital storage media continue to grow exponentially[6] with competitive markets that drive sales prices down. As of June 2009, the U.S. accounts for over 22 percent (over 264 million) of all personal computers in the world (over 1.19 billion)[7], but China recently surpassed the U.S. in number of Internet users (253 million vice 220 million).[8] With 222 countries having Internet access, 86 of which have at least one million users,[9] it is becoming difficult to find any place in the world not affected by cyberspace.

Since the cyberspace process includes physical elements, it is not surprising that industry and government leverage the ability of cyberspace-based remote access to control infrastructure. Usually called Supervisory Control and Data Acquisition (SCADA) systems, these control processes increase operational effectiveness and efficiency for many applications to include such systems as electric power, oil, gas, transportation, and telecommunications.[10] Often, older SCADA devices were designed and installed without regard for security, and most new SCADA systems use the Internet to pass control information. As the worldwide population of Internet users pushes toward two billion, it is wise to pursue better security promptly for any physical systems accessible via that portion of cyberspace.[11]

b. Threats. What types of threats exist in this new common? In general, attacks in cyberspace fall into one of three categories—the interception, modification, or denial of information.[12] Attacks may be overt or covert with kinetic or non-kinetic effects. The damage inflicted varies greatly--from defaced websites, to multi-million-dollar financial losses, and even to actual physical damage to equipment whose control is connected to cyberspace.

Who are the perpetrators of illegal activity in cyberspace? The vast diversity of cyberspace lawbreakers can be divided into four categories of individuals (who may also work in groups)—cyber-delinquents, cyber-criminals, cyber-spies, and cyber-terrorists. Each set of perpetrators differs in their attitudes and actions regarding ideology (e.g., political or religious), monetary gain, attribution, knowledge sharing, and destruction of societal structures. One common interest among all but the most extreme individuals (e.g., anarchists) is the preservation of cyberspace infrastructure—they all have a vested interest in maintaining the domain from which they derive power.

Individuals in the four broad categories of cyberspace wrongdoers may interact for mutual benefit or they may exploit law-abiding operators. There are documented cases where cyber-terrorists employed cyber-criminals to steal credit card information and support drug traffickers, all toward the goal of funding traditional terrorist operations. Another lucrative business is the marketing of "botnets," virtual armies of compromised computers that can be controlled remotely over the Internet by a "botmaster". Botnets may exploit hundreds of thousands of computers, usually without the owners' knowledge.[13] An adversary with such capability, if coupled with a network structure, could achieve swarming attacks and defenses—in cyberspace as well as other strategic commons—that challenge the "traditional mass- and maneuver-oriented approaches to conflict."[14]

What is less clear is how state and nonstate actors are using cyberspace to pursue strategic goals. The continuing advances in cyberspace "will be available to America's opponents, who will use them to attack, degrade, and disrupt communications and the flow of information."[15] Among these potential state and nonstate adversaries, China's emerging military capabilities in cyberspace reflect an asymmetrical approach consistent with the classical Chinese strategic thinkers.[16]

3. Cyberspace and Instruments of National Power.

a. Diplomatic. How should countries interact in cyberspace? Does this new common require entirely new standards of conduct? As independent governments, countries have an international obligation to act in good faith and settle disputes with other states by peaceful means. If conflict should occur, the right of using proportional force in self-defense is a cornerstone of international security. Legal experts argue that "it now seems almost universally accepted that a considerable body of international law does indeed apply to the use of force by states in CyberSpace."[17]

However, the widely distributed nature of cyberspace does not necessarily recognize national boundaries, and new provisions to address this reality seem prudent. Arguably, the most significant event toward defining acceptable cyberspace interactions is the Council of Europe Convention on Cybercrime, a formal agreement among 43 countries "to better combat cybercrime by harmonizing national laws, improving investigative abilities, and boosting international cooperation."[18] The convention began in 1997, was opened for signature on November 23, 2001, and has been ratified by at least 26 countries.[19] Its provisions include definition of criminal offenses in four categories (fraud and forgery, child pornography, copyright infringement, and security breaches) as well as methods to address these crimes, such as investigation and extradition procedures.[20]

The U.S. Department of Justice has arrested and convicted domestic and international individuals and small groups committing cyberspace-related crimes since 1998.[21] The department determines whether the crime targeted a private individual or corporation, or a government agency as well as whether the crime posed a threat to public health or safety (i.e., power grids, air traffic control, etc.).[22] The attackers include citizens from China, Russia, Kazakhstan, Israel, and the United Kingdom. In some cases, extradition requests were pursued per the Convention on Cybercrime.[23]

b. Information. How can information be stored safely in cyberspace? The U.S. government views information technology (IT) as one sector of the nation's critical infrastructure, and has tasked the Department of Homeland Security (DHS) to direct its protection. In turn, DHS created a National Cyber Security Division in June 2003 to serve as a focal point for cybersecurity issues. Working to avoid information sharing failures that contributed to the September 2001 terrorist attacks, HLS conducted 16 major cyber exercises between 2004 and 2008. To practice and enhance collective responses to cybersecurity scenarios, the exercises included participants from federal, state, and local governments as well as ones from private industry, academic institutions, and foreign governments.[24]

In January 2008, President Bush signed Homeland Security Presidential Directive 23, better known as the Comprehensive National Cybersecurity Initiative (CNCI). The CNCI is a classified document, but three of its major "public" priorities directly support the access points, data traffic, and security protocol for information traversing U.S. government agencies' computer networks. First, the Trusted Internet Connection effort is simply a way to prevent cyber attacks by reducing the number of access points. Next, the Einstein II program automatically monitors the data traffic within the networks and Internet access points. Third, the Federal Desktop Core Configuration program mandates a common security protocol for government desktop computer systems.[25]

In May 29, 2009, President Obama announced the creation of a new White House office led by a Cybersecurity Coordinator as well as five key areas for action. The coordinator will be a member of both the National Security Staff and the National Economic Council. As of November 1, 2009, this position remains unfilled by the administration.[26] However, on October 30, 2009, DHS Secretary Napolitano opened the new National Cybersecurity and Communications Integration Center (NCCIC), a 24-hour watch and warning center to identify and mitigate risks that could disrupt or degrade critical U.S. cyberspace infrastructure. The NCCIC combines two DHS operational organizations: the Computer Emergency Readiness Team and the National Coordinating Center for Telecommunications.[27]

c. Economic. What are the costs to industry of cybersecurity breaches? The stakes are high—a recent report surveying senior IT decision makers from over 1,000 large businesses and security firms estimated that companies lost an average of 4.6 million dollars (U.S.) worth of intellectual property in 2008.[28] The latest Annual Threat Assessment of the Intelligence Community estimates total cyber-related business losses in 2008 to be 42 billion dollars for the U.S. and 140 billion dollars globally, as well as possibly one trillion dollars worth of intellectual property lost globally.[29] Even determining when an attack occurs in business is difficult, and it is even more challenging to measure the cost of attacks. However, investigations into stock price impacts following cyber-attacks indicate that targeted firms suffer short-term losses of one to five percent—such drops could translate into shareholders losses as much as 200 million dollars.[30]

d. Military. How are traditional military organizations embracing operations within the cyberspace domain? In his recent testimony before the U.S. Congress, Secretary of Defense Robert Gates acknowledged the extent of the threat:

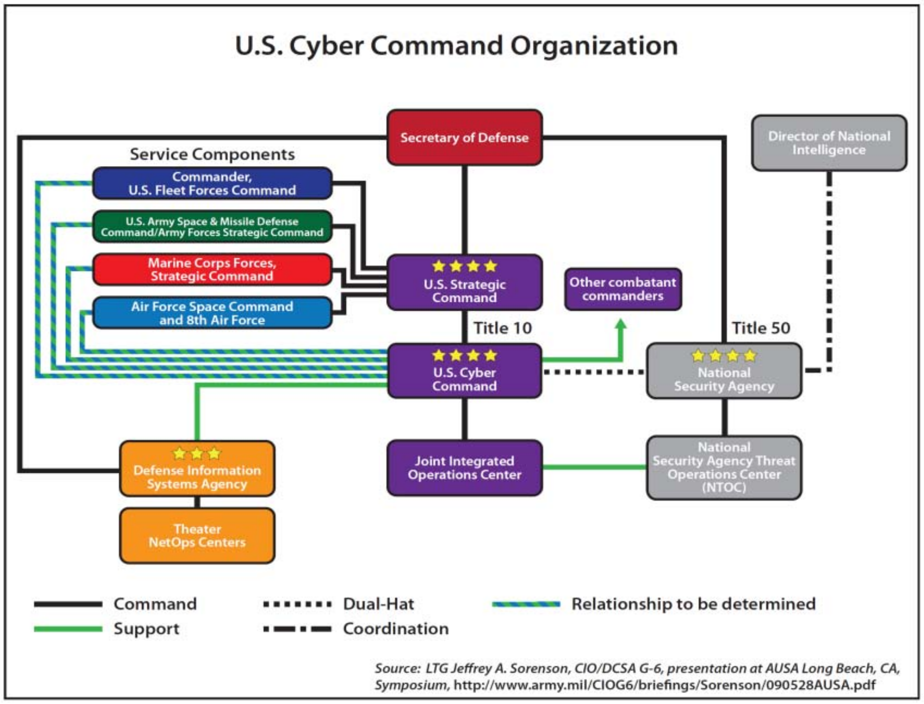
> *With cheap technology and minimal investment, current and potential adversaries operating in cyberspace can inflict serious damage to DoD's vast information grid—a system that encompasses more than 15,000 local, regional, and wide-area networks, and approximately 7 million IT devices.*[31]

To address this issue, Secretary Gates designated cyberspace as one of the four focus areas in the recent Quadrennial Roles and Missions Review, a reinforcement of tenets in his 2008 National Defense Strategy.[32] The goal is to establish the foundation to develop capable cyberspace forces, structure them as well as their processes and procedures, and then employ these forces to achieve desired effects across the full range of military operations. The study's Cyber Issue Team emphasized the need "to learn from new, innovation capabilities and experiences of our counterparts across the U.S. Government, in the private sector, and internationally."[33]

In April 2007, the Estonian government, commercial and private organizations endured three weeks of cyber attacks. Responding to an historic request by a member state of the North Atlantic Treaty Organization (NATO) in defense of its digital assets, the U.S. sent computer security experts to Estonia to help with recovery efforts.[34] The aftermath of this attack included the creation of two new cybersecurity organizations. First, at the operational level, the Cyber Defence Management Authority (CDMA) was established in Brussels, Belgium, to provide a centralized bureau for coordinating Alliance response to any further cyber attacks.[35] Second, at the strategic level, the Cooperative Cyber Defense Center of Excellence (CCD CoE) was established at Tallinn, Estonia, with a mission "to enhance the cooperative cyber defence capability of NATO and NATO nations, thus improving the Alliance's interoperability in the field of cooperative cyber defence."[36]

In August 2008, the movement of Russian tanks into Georgia was accompanied with several distributed denial of service attacks on Georgian websites. While there may be no conclusive evidence proving that the cyber attacks were carried out or sanctioned by the Russian government, the coincidence of the timing with the conventional attacks cannot be ignored.[37]

On June 23, 2009, Secretary of Defense Gates directed the development of a new national strategy for cybersecurity as well as the establishment of U.S. Cyber Command (USCYBERCOM) as a subordinate unified command under U.S. Strategic Command. He specified an initial operating capability not later than October 2009, and full operating capability by October 2010. The mission, roles, and responsibilities of the new command are still in development. However, its structure will include service components as well as support from the Defense Information Systems Agency (DISA). It will have Title 10 and Title 50 responsibilities using a dual-hat structure with the commander, USCYBERCOM also serving as director, National Security Agency (NSA)(see Figure 2.). The existing Joint Task Force-Global Network Operations (JTF-GNO) and Joint Functional Component Commander-Network Warfare (JFCC-NW) will be disestablished and their missions will be subsumed into USCYBERCOM.[38]


U.S. Cyber Command Organization
Secretary of Defense
Director of National Intelligence
Service Components
Commander, U.S. Fleet Forces Command
U.S. Army Space & Missile Defense Command/Army Forces Strategic Command
Marine Corps Forces, Strategic Command
Air Force Space Command and 8th Air Force
★★★★ U.S. Strategic Command
Other combatant commanders
Title 10
Title 50
★★★★ U.S. Cyber Command
★★★★ National Security Agency
★★★ Defense Information Systems Agency
Joint Integrated Operations Center
National Security Agency Threat Operations Center (NTOC)
Theater NetOps Centers
Command
Support
Dual-Hat
Coordination
Relationship to be determined

Source: LTG Jeffrey A. Sorenson, CIO/DCSA G-6, presentation at AUSA Long Beach, CA, Symposium, http://www.army.mil/CIOG6/briefings/Sorenson/090528AUSA.pdf

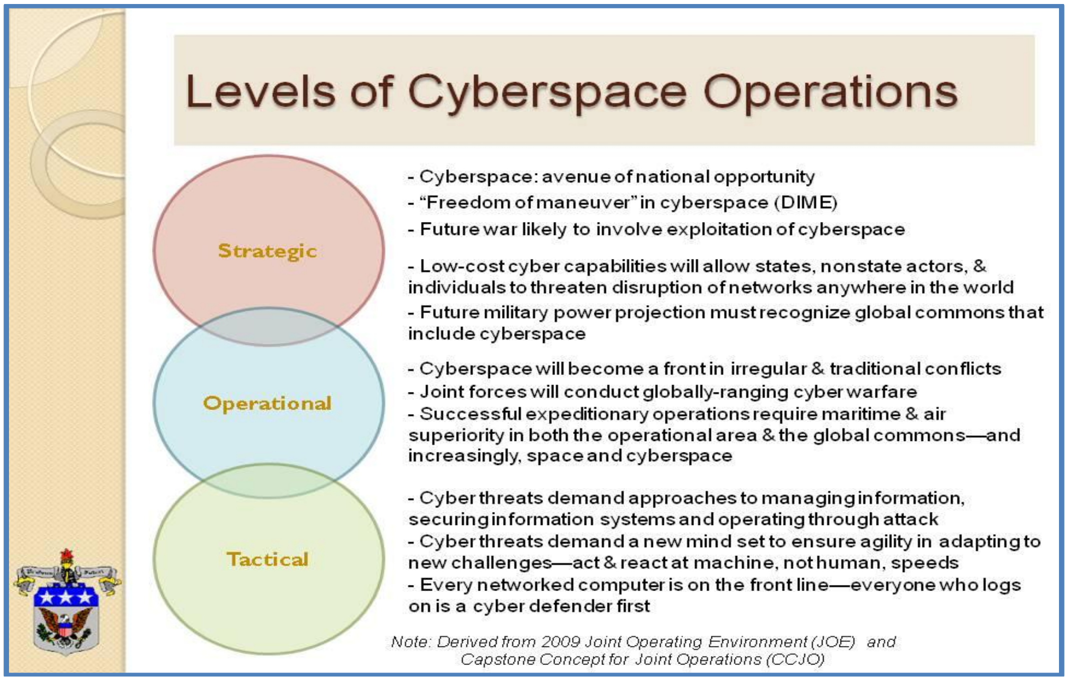
Figure 2. Notional U.S. Cyber Command Organization[39]

4. Cyberspace Operations Issues.[40]

a. Cyberspace Operations in the Joint Operating Environment (JOE). The 2008 JOE describes the challenges facing the future joint force across a wide range of threats and opportunities which include "sustained engagement in the global commons," which include cyberspace.[41] The ongoing trend of significant improvement in cyber-related technologies will continue to change how military operations are conducted at the tactical, operational, and strategic levels. The January 2009 *Capstone Concept for Joint Operations* (CCJO) further elaborates on the changing nature of cyberspace in joint operations, providing broad precepts and assertions to help guide the development and employment of future joint forces.

Figure 3 provides a summary of many of the key concepts of cyberspace operations espoused within the JOE and CCJO. One overarching concept is the envisioned emergence of cyberspace as a global common that demands freedom of maneuver at the strategic level as well as localized domain superiority as a requisite for successful future expeditionary operations.[42] Also, there is a consistent expectation that future conflict will not only include cyberspace operations, but also that the cyberspace common itself may become a main front in both irregular and traditional conflict.

b. War in Cyberspace. If the projections of the JOE and CCJO come to fruition and cyberspace becomes a hotly contested global common, will this require new definitions for war and deterrence? This question is being debated and no consensus answer has emerged yet. There is no internationally accepted definition of when hostile actions in cyberspace are recognized as attacks, let alone acts of war. However, scholars are making progress in this area, such as the application of an analytical framework developed by Professor Michael Schmitt that attempts to determine if a cyber attack equates to the use of force in accepted terms of the United Nations.[43] The Schmitt Analysis considers the intensity of damage in each of seven areas (severity, immediacy, directness, invasiveness, measurability, presumptive legitimacy, and responsibility) to provide a composite assessment of the effects of the cyber attack.[44]



Levels of Cyberspace Operations

- Cyberspace: avenue of national opportunity
- "Freedom of maneuver" in cyberspace (DIME)
- Future war likely to involve exploitation of cyberspace
- Low-cost cyber capabilities will allow states, nonstate actors, & individuals to threaten disruption of networks anywhere in the world
- Future military power projection must recognize global commons that include cyberspace
- Cyberspace will become a front in irregular & traditional conflicts
- Joint forces will conduct globally-ranging cyber warfare
- Successful expeditionary operations require maritime & air superiority in both the operational area & the global commons—and increasingly, space and cyberspace
- Cyber threats demand approaches to managing information, securing information systems and operating through attack
- Cyber threats demand a new mind set to ensure agility in adapting to new challenges—act & react at machine, not human, speeds
- Every networked computer is on the front line—everyone who logs on is a cyber defender first

Note: Derived from 2009 Joint Operating Environment (JOE) and Capstone Concept for Joint Operations (CCJO)

Figure 3. Levels of Cyberspace Operations[45]

c. <u>Cyberspace Theory Development.</u> In general, theory provides the overarching abstract thought and philosophical foundation necessary to analyze a given concept with appropriate rigor. Given the model of cyberspace as a global common, what is the best approach to develop its theory of operation? A valuable analogy is that of traditional (i.e., Mahan) naval theory, part of which involves the difference between naval operations in the littoral area—the "brown water"—versus those in the broad ocean area—the "blue water." Simply put, when one connects the major ports in the "brown water" to other ports in the world, "sea lines of communication" emerge that have strategic importance based on many factors including geography and volume of traffic.[46]

Similarly, cyberspace can be mapped using techniques that clearly show its "cyber lines of communication" and critical nodes with tactical, operational, and strategic implications for their control.[47] When combined with innovative graphical depictions, these maps clearly show nodes and choke points—the "blue water cyberspace" equivalent of the Straits of Malacca.[48] The security of these critical nodes—some of which may be physical, others informational—should be of great interest to anyone attempting to protect or exploit cyberspace. Unfortunately, openly espoused cyberspace efforts often seem to focus on "brown water cyberspace," thus relegating a critical area of future operations to the mere tactics, techniques, and procedures of passwords, firewalls, and antivirus checks. While these measures do offer crucial protection in the "brown water cyberspace" where most operators work, they become less effective when data packages traverse the "cyberspace blue waters" in route to their planned destination, often an area of "brown water cyberspace" not under the control of the sender or even the sender's country or organization.

5. Conclusion.

Cyberspace is a modern embodiment of an enduring process, accelerated by technology, that combines cognitive, physical, and information elements. Cyberspace has significant influences on, and implications for, all instruments of national power. The national security aspects of cyberspace are still evolving with DHS focusing on defensive efforts and DoD working toward a more holistic security approach organized within a new subunified command. However, much work remains in the practical definitions of war and deterrence in cyberspace as well as the development of fundamental cyberspace theory. Strategic leaders should study and embrace implications of the rapidly growing role of cyberspace operations in future conflict. Such operations currently fulfill supporting roles, but in time, they may become a main front of war itself.

Colonel Jeff Caton, USAF
Information in Warfare Group
Department of Command, Leadership, and Management
U.S. Army War College

(Current as of 31 October 2009)

[1] U.S. Deputy Secretary of Defense Gordon England, "The Definition of 'Cyberspace'," memorandum for Secretaries of the Military Departments, Washington, DC, May 12, 2008.

[2] Arthur K. Cebrowski, "Transformation and the Changing Character of War?" *Transformation Trends*, June 17, 2004, http://www.afei.org/transformation (accessed 27 March 2009).

[3] Pamela L. Woolley, *Defining Cyberspace as a United States Air Force Mission,* Graduate Research Project (Wright-Patterson Air Force Base, OH: Air Force Institute of Technology, June 2006), 8.

[4] Jeffrey L. Caton, *What do Senior Leaders Need to Know about Cyberspace*, Paper (Kista, Sweden: International Transformation Conference, June 3, 2009).

[5] Cebrowski, 7.

[6] Magnus Ekman et al., *An In-Depth Look at Computer Performance Growth*, Technical Report 2004-9 (Goteborg: Chalmers University of Technology, 2004).

[7] "PCs In-Use Reached nearly 1.2B in 2008; USA Accounts for Over 22% of PCs In-Use," News Release (*Computer Industry Almanac, Inc.* January 14, 2009). http://www.c-i-a.com (accessed 31 March 2009).

[8] *Top 20 Countries with the Highest Number of Internet Users*, Internet World Stats. http://www.internetworldstats.com (accessed 31 March 2009).

[9] "Country Comparisons—Internet Users," *The World Factbook* (Washington, DC: Central Intelligence Agency, 2008), https://www.cia.gov/library/publications (accessed 31 March 2009).

[10] Samuel G. Varnado, "SCADA and the Terrorist Threat: Protecting the Nation's Critical Control Systems," (Washington, DC: U.S. House of Representatives, October18, 2005).

[11] "Experiment Showed Grid Vulnerability to Cyber Attack – Flaws Fixed," *Energy Assurance Daily* (Washington, DC: U.S. Department of Energy, September 27, 2007). http://www.oe.netl.doe.gov/ (accessed 7 May 2009). The U.S. Department of Energy reported on recommended changes to power generation facilities resulting from a U.S. Department of Homeland Security experiment in March 2007. The test demonstrated the ability to cause catastrophic physical damage to an industrial turbine via commands sent through its SCADA system.

[12] Woolley, 32.

[13] Clay Wilson, Botnets, *Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress*, CRS Report for Congress RL-32114 (Washington, DC: Congressional Research Service, January 29, 2008).

[14] John Arquilla and David Ronfeldt, "The Advent of Netwar (Revisited)," in *Networks and Netwars* (Santa Monica: RAND, 2001), 12.

[15] U.S. Joint Forces Command, *Joint Operating Environment (JOE)* (Norfolk, VA: U.S. Joint Forces Command, November 25, 2008), 23.

[16] Ibid, 27. For more information on Chinese strategic thought in cyberspace issues, recommend Timothy L. Thomas, *Decoding the Virtual Dragon: Critical Evolutions in the Science and Philosophy of China's Information Operations and Military Strategy* (Fort Leavenworth, KS: Foreign Military Studies Office, 2007).

[17] Walter G. Sharp, *CyberSpace and the Use of Force* (Falls Church: Aegis Research.Sharp, 1999).

[18] Kristin Archick, *Cybercrime: The Council of Europe Convention*, CRS Report for Congress RS21208 (Washington, DC: Congressional Research Service, September 28, 2006), 1.

[19] "Convention on Cybercrime Status of Signatures and Ratifications" (Council of Europe, September 11, 2009) http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG (accessed November 9, 2009). Note that in addition to the 26 countries that have ratified the convention, 20 additional countries are non-ratified signatories.

[20] Archick, 2.

[21] The fact that the U.S. Department of Justice claims jurisdiction for cyberspace crimes having physical impacts on U.S. individuals and organizations is not the same as suggesting there is a "U.S. cyberspace boundary." However, the details of physical and virtual national sovereignty deserve further debate beyond this article's scope.

[22] Department of Justice, *Computer Crime Cases* (Washington: Department of Justice) http://www.cybercrime.gov/cccases.html (accessed 24 March 2009).

[23] Department of Justice, *London, England Hacker Indicted Under Computer Fraud and Abuse Act for Accessing Military Computers* (Washington, DC: Department of Justice, 2009) http://cybercrime.gov/mckinnonIndict.htm (accessed 24 March 2009).

[24] U.S. Government Accountability Office, *Critical Infrastructure Protection: DHS Needs to Fully Address Lessons Learned from Its First Cyber Storm Exercise* (GAO-08-825), (Washington, DC: Government Accountability Office, September 2008). Cyber Storm II description: Sponsored by DHS, this exercise was to improve national incident response and coordination capabilities by simulating physical and cyber attacks against the transportation, information technology, and chemical critical infrastructure sectors. Participants included federal, state, and foreign governments and private industry.

[25] Brian Lake, "CyberThreats: A Cultural Change of Combating Threats," *Homeland Defense Journal* 6 no. 7 (December 2008): 14-16.

[26] Barack Obama, *Remarks by the President on Securing Our Nation's Cyber Infrastructure* (Washington DC: The White House, May 29, 2009). The five areas of emphasis for cybersecurity by the President were: new comprehensive strategy; organized and unified response; strengthen public/private partnership; cutting-edge research and development; and promote cybersecurity awareness and "digital literacy." It is interesting to note that President Obama mentioned that his staff's computers were hacked during the general election campaign.

[27] Department of Homeland Security, *Secretary Napolitano Opens New National Cybersecurity and Communications Integration Center*, Press Release (Washington DC: Department of Homeland Security, October 30, 2009) http://www.dhs.gov/ynews/releases/pr_1256914923094.shtm (accessed November 9, 2009).

[28] *Unsecured Economies: Protecting Vital Information* (Santa Clara: McAfee, 2009).

[29] U.S. Director of National Intelligence Dennis C. Blair, *Annual Threat Assessment of the Intelligence Community for the House Permanent Select Committee on Intelligence* (Washington, DC: Director of National Intelligence, February 25, 2009).

[30] Brian Cashell et al., *The Economic Impact of Cyber-Attacks*, CRS Report for Congress RL-32331 (Washington, DC: Congressional Research Service, April 1, 2004).

[31] U.S. Secretary of Defense Robert M. Gates, *Submitted Statement to Senate Armed Services Committee* (Washington, DC: U.S. Senate, January 27, 2009), 8.

[32] U.S. Secretary of Defense Robert M. Gates, *Quadrennial Roles and Missions Review Report* (Washington, DC: Department of Defense, January 2009) and *National Defense Strategy* (Washington, DC: Department of Defense, June 2008).

[33] Gates, *Quadrennial Roles and Missions Review Report* , 14-16. The stated DoD vision is to develop cyberspace capability that provides global situational awareness of cyberspace, U.S. freedom of action in cyberspace, the ability to provide warfighting effects within and through cyberspace, and, when called upon, provide cyberspace support to civil authorities.

[34] Kenneth Geers, *Cyberspace and the Changing Nature of Warfare,* Report IST-076/RSY-017 (Tallinn, Estonia: Cooperative Cyber Defence Centre of Excellence, 2008).

[35] Rex B. Hughes, "NATO and Cyber Defence: Mission Accomplished?" *Atlantisch Perspectief* 1 no. 4: 4-8.

[36] Cooperative Cyber Defence Centre of Excellence, *Mission and Vision* (Tallinn, Estonia: Cooperative Cyber Defence Centre of Excellence). http://transnet.act.nato.int/WISE/TNCC/CentresofE/CCD (accessed 30 March 2009).

[37] "Marching off to Cyber War," *The Economist* (print edition), December 4, 2008.

[38] U.S. Secretary of Defense Robert M. Gates, "Establishment of a Subordinate Unified U.S. Cyber Command Under U.S. Strategic Command for Military Cyberspace Operations," memorandum for Secretaries of the Military Departments, Washington, DC, June 23, 2009.

[39] Richard Mereand, *Securing Cyberspace: Guarding the New Frontier* (Arlington, VA: Association of the United States Army Institute of Land Warfare, August 25, 2009), 4. For additional information on the Army G-6 efforts in this area, see LTG Jeffrey A. Sorenson, *C4, Space & Cyber: Enabling the Global Network Enterprise Construct* (Long Beach, CA: Association of the United States Army, May 28, 2009) and other related briefs at http://www.army.mil/ciog6/briefings.html (accessed November 9, 2009).

[40] Cyberspace operations are defined for DoD as "The employment of cyber capabilities where the primary purpose is to achieve military objectives or effects in and through cyberspace. Such operations include computer network operations and activities to operate and defend the Global Information Grid." This also includes combatant commander consideration to use cyberspace operations as a means to achieve strategic or tactical objectives with effects in any domain. See: Vice Chairman of the Joint Chiefs of Staff General James E. Cartwright, "Definition of Cyberspace Operations," action memorandum for Deputy Secretary of Defense, Washington DC, September 29, 2008 (endorsed as approved on October 15, 2008).

[41] *Joint Operating Environment (JOE),* 3, 44.

[42] *Capstone Concept for Joint Operations (CCJO), Version 3.0* (Washington, DC: Department of Defense, January 15, 2009), 26, 31.

[43] Scott W. Beidleman, *Defining and Deterring Cyber War,* Strategy Research Project (Carlisle Barracks, PA: U.S. Army War College, June 1, 2009), 2.

[44] James B. Michel et al., "Measured Responses to Cyber Attacks Using Schmitt Analysis: A Case Study of Attack Scenarios for a Software-Intensive System," *Proceedings of Twenty-seventh Annual International Software and Applications Conference* (Dallas, TX: Institute of Electrical and Electronics Engineers, November, 2003).

[45] Figure 3 consists of summarized excerpts from the *Joint Operating Environment (JOE)* and the *Capstone Concept for Joint Operations (CCJO), Version 3.0.*

[46] A.T. Mahan, *The Influence of Sea Power Upon History 1660-1783* (Mineola, NY: Dover, 1987 reprint), p 30: "The geographical position of a county may not only favor the concentration of its forces, but give the further strategic advantage of a central position and a good base for hostile operations against its probable enemies." p.31-32: "If, in addition to facility for offence, Nature has so placed a country that it has easy access to the high sea itself, while at the same time it controls one of the greatest thoroughfares of the world's traffic, it is evident that the strategic value of its position is very high."

[47] Martin Dodge and Rob Kitchin, *Atlas of Cyberspace* (Harlow, UK: Pearson Education Limited, 2001). Dodge and Kitchin conducted a 5-year study of cyberspace maps and spatializations created by academic and commercial organizations, and compiled their results in *Atlas of Cyberspace*. Also, the Cooperative Association for Internet Data Analysis (CAIDA) in San Diego is pioneering the macroscopic measurement and analysis of Internet performance, developing several practical maps of topology, security, routing, and other aspects. See K. Claffy et al., *Internet Mapping: from Art to Science* (San Diego, CA: Cooperative Association for Internet Data Analysis, 2008) and *Data Collection at CAIDA—*

Research Topics (San Diego, CA: Cooperative Association for Internet Data Analysis, 2009). http://www.caida.org/data/ (accessed 31 March 2009).

[48] *Joint Operating Environment (JOE)*, 27. China's energy security is dependent on freedom of navigation through the Straits of Malacca, through which travels 80% of their oil imports.

This Page Intentionally Blank

Strategic Communication: Organizations & Concepts

Office of the Deputy Secretary of Defense for Public Affairs, Joint Communication DASD(JC)

Strategic Communication (SC) comprises the focused processes and efforts to understand and engage key audiences to create, strengthen, or preserve conditions favorable to advance national interests and strategic objectives by coordinating actions and information, synchronized with other elements of national power. *(This is the revised definition submitted for inclusion in the next update to Joint Publication 5-0, Joint Operation Planning.)*

SC is a natural extension of strategic direction, and supports the President's strategic guidance, the National Defense Strategy, and the National Military Strategy. SC planning establishes unity of US themes and messages, emphasizes success, accurately confirms or refutes external reporting on US operations, and reinforces the legitimacy of US goals. This is an interagency effort, which provides an opportunity to advance US regional and global partnerships. (JP 5-0)

At its most basic, SC is the orchestration of actions, images, and words to achieve desired effects. SC is the process of coordinating horizontally (across DoD and the US Government, as well as with international partners as appropriate) and vertically (up and down the chain of command) to:

- close the "say-do gap";
- consider information and communication as part of strategy, planning and policy development from the very beginning;
- assess communication impacts of actions before taking actions; and
- consider "soft power" capabilities equally with more traditional DoD kinetic capabilities when determining the optimum course of action.

SC planning goes beyond a single operation or bilateral engagement, focusing on the region, operating environment and globe. It's also less about "sending a message" and more about engagement. More than ever, efforts to listen to and understand different perspectives and cultures must be deliberately planned and integrated into the decision cycle of all diplomats and joint force commanders to ensure America's future success.

Note: SC exists primarily as a DoD term. Though DoS sometimes uses "SC" as an overarching concept, they most often recognize SC as parallel to Public Diplomacy (PD). The guiding (even if outdated) USG-level document is titled "U.S. National Strategy for Public Diplomacy and Strategic Communication" and the Under Secretaries of State for Public Diplomacy and Public Affairs have generally used "Public Diplomacy and Strategic Communication" or "SC and PD."

DASD(JC) was created in December 2005 to assist the ASD(PA) in shaping DoD-wide processes, policy, doctrine, organization, and training of the primary communication supporting capabilities, particularly public affairs and visual information. DASD(JC) has assumed many of the strategic communication planning responsibilities and functions previously performed by the Strategic Communication Integration Group (SCIG) Secretariat, disbanded in early 2008.

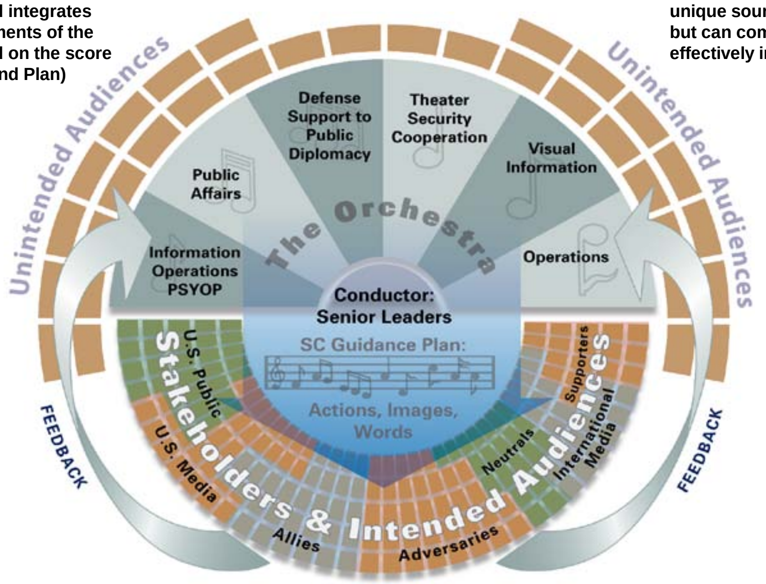
DASD(JC) leads communication integration and planning on strategic issues and mid- to long-range efforts, to ensure that communication plans and strategies are coordinated and synchronized across the Department and with other USG agencies, and that ASD(PA) equities are represented, to maximize DoD's capability to communicate in an aggressive and synchronized manner.

This Page Intentionally Blank

This Page Intentionally Blank

SC is like an orchestra producing harmony

- Conductor (Senior Leader) coordinates and integrates the various elements of the orchestra based on the score (SC Guidance and Plan)
- All instruments retain their unique sound and specialty, but can communicate more effectively in concert



The selection, timing, and emphasis of SC instruments help orchestrate the message to stakeholders consistent with a desired effect or commander's intent. The Conductor must continuously adapt the score based on stakeholder feedback.

When discussing SC, we use this orchestra analogy. We welcome and encourage you to use it, as appropriate.

Analogy of SC as an orchestra, with:

- Conductor = Senior Leaders
- Musical Score = SC plan
- Orchestra = the various SC communities of practice &/or lines of operation
- Music = coordinated and synchronized actions, images, & words
- Audience = communication based on the intended effect on the audience (for ex: the mood you want to achieve is based on the type of music you play; jazz, rock, country, etc.)

Similar to delivering a successful concert, SC is about orchestrating all our military capabilities to achieve our desired effects. Sometimes the effect we desire will require integrating PSYOP-developed radio programming and handbills with engineering skills to build schools and wells; sometimes the emphasis will be on leader engagement to listen and understand (before talking); and sometimes it will take a very loud drum (kinetic action) to achieve the desired effect.

Keep in mind the rehearsals can be difficult and messy! But necessary!

Last Updated: October 2009

This Page Intentionally Blank

Principles of Strategic Communication

August 2008

15 August 2008

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Principles of Strategic Communication Guide

Strategic Communication has been viewed as an emerging and extremely pertinent joint concept in recent years. Several important review panels have addressed Strategic Communication (SC) and the Chairman of the Joint Chiefs of Staff has designated Strategic Communication as one of the CJCS Special Areas of Emphasis for joint education in 2007 and 2008.

Despite the interest and attention, Strategic Communication is still a developing concept. Contributing to the challenge is the lack of approved policy and doctrine.

As part of a larger DoD Strategic Communication education initiative, the Department held the first Strategic Communication Education Summit in March 2008, at the Joint Forces Staff College in Norfolk, Va. One of the most significant outcomes was the development of "Principles of Strategic Communication" to help standardize Strategic Communication education until policy and doctrine are published.

Through the collaborative efforts of DoD, State Department, and civilian educators and practitioners, the Principles initially developed in the Strategic Communication Education Summit have been refined into this guide. The purpose of this publication is to provide a tool to assist dialogue and instruction promoting understanding Strategic Communication.

As the Strategic Communication concept continues to mature, these Principles will be reviewed every two years until they are incorporated into formal doctrine. Comments are welcome and should be addressed to the Office of the Deputy Assistant Secretary of Defense for Joint Communication.

Robert T Hastings

Robert T. Hastings
Principal Deputy Assistant Secretary
of Defense for Public Affairs

DISTRIBUTION:
SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF JOINT CHIEFS OF STAFF
SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
COMMANDERS OF THE COMBATANT COMMANDS
ASSISTANT SECRETARIES OF DEFENSE
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTORS OF DEFENSE AGENCIES
DIRECTORS OF DOD FIELD ACTIVITIES
COMMANDANTS OF THE JOINT MILITARY EDUCATIONAL INSTITUTIONS

Principles of Strategic Communication

Definition of a principle: *A fundamental tenet; a determining characteristic; an essential quality; an enduring attribute.*

Strategic Communication (SC) has been described as the orchestration and/or synchronization of actions, images, and words to achieve a desired effect, yet there is more to understanding the concept.

As the joint force and agencies of the U.S. Government have begun executing Strategic Communication processes, common fundamentals have emerged. Through the collaborative efforts of DoD, State Department, civilian educators, and Strategic Communication practitioners, those common fundamentals have been consolidated and refined into nine principles of SC, described below. These principles are provided to assist dialogue and instruction promoting understanding of Strategic Communication.

Figure 1 below lists the nine principles of SC, with a short description of each. A more detailed explanation of each principle follows. The principles are not listed in any order of precedence.

Leadership-Driven
Leaders must lead communication process

Credible
Perception of truthfulness and respect

Dialogue
Multi-faceted exchange of ideas

Unity of Effort
Integrated and coordinated

Responsive
Right audience, message, time, and place

Understanding
Deep comprehension of others

Pervasive
Every action sends a message

Results-Based
Tied to desired endstate

Continuous
Analysis, Planning, Execution, Assessment

Figure 1. Principles of Strategic Communication

Leadership-Driven. Leaders must decisively engage and drive the Strategic Communication process.

To ensure integration of communication efforts, leaders should place communication at the core of everything they do. Successful Strategic Communication – integrating actions, words, and images – begins with clear leadership intent and guidance. Desired objectives and outcomes are then closely tied to major lines of operation outlined in the organization, command or joint campaign plan. The results are actions and words linked to the plan. Leaders also need to properly resource strategic communication at a priority comparable to other important areas such as logistics and intelligence.

Credible. Perception of truthfulness and respect between all parties.
Credibility and consistency are the foundation of effective communication; they build and rely on perceptions of accuracy, truthfulness, and respect. Actions, images, and words must be integrated and coordinated internally and externally with no perceived inconsistencies between words and deeds or between policy and deeds. Strategic Communication also requires a professional force of properly trained, educated, and attentive communicators. Credibility also often entails communicating through others who may be viewed as more credible.

Understanding. Deep comprehension of attitudes, cultures, identities, behavior, history, perspectives and social systems. What we say, do, or show, may not be what others hear or see.
An individual's experience, culture, and knowledge provide the context shaping their perceptions and therefore their judgment of actions. We must understand that concepts of moral values are not absolute, but are relative to the individual's societal and cultural narrative. Audiences determine meaning by interpretation of our communication with them; thus what we say, do, or show, may not be what they hear or see. Acting without understanding our audiences can lead to critical misunderstandings with serious consequences.

Understanding subjective impacts of culture, language, history, religion, environment, and other factors is critical when crafting communication strategy for a relevant population. Building relationships and collaboration with the interagency, coalition, host nation, academic, non-profit, and business communities can facilitate better understanding of audiences.

Dialogue. Multi-faceted exchange of ideas to promote understanding and build relationships.
Effective communication requires a multi-faceted dialogue among parties. It involves active listening, engagement, and the pursuit of mutual understanding, which leads to trust. Success depends upon building and leveraging relationships. Leaders should take advantage of these relationships to place U.S. policies and actions in context prior to operations or events. Successful development and implementation of communication strategy will seldom happen overnight; relationships take time to develop and require listening, respect for culture, and trust-building.

Pervasive. Every action, image, and word sends a message.
Communication no longer has boundaries, in time or space. All players are communicators, wittingly or not. Everything the Joint Force says, does, or fails to do and say, has intended and unintended consequences. Every action, word, and image sends a message, and every team member is a messenger, from the 18-year-old rifleman to the commander. All communication can have strategic impact, and unintended audiences are unavoidable in the global information environment; therefore, leaders must think about possible "Nth" order communication results of their actions.

Unity of Effort. Integrated and coordinated, vertically and horizontally.
Strategic Communication is a consistent, collaborative process that must be integrated vertically from strategic through tactical levels, and horizontally across stakeholders. Leaders coordinate and synchronize capabilities and instruments of power within their area of responsibility, areas of influence, and areas of interest to achieve desired outcomes. Recognizing that your

agency/organization will not act alone, ideally, all those who may have an impact should be part of communication integration.

Results-Based. Actions to achieve specific outcomes in pursuit of a well-articulated endstate.
Strategic communication should be focused on achieving specific desired results in pursuit of a clearly defined endstate. Communication processes, themes, targets and engagement modes are derived from policy, strategic vision, campaign planning and operational design. Strategic communication is not simply "another tool in the leader's toolbox," but must guide all an organization does and says; encompassing and harmonized with other functions for desired results.

Responsive. Right audience, right message, right time, and right place.
Strategic Communication should focus on long-term end states or desired outcomes. Rapid and timely response to evolving conditions and crises is important as these may have strategic effects. Communication strategy must reach intended audiences through a customized message that is relevant to those audiences. Strategic Communication involves the broader discussion of aligning actions, images, and words to support policy, overarching strategic objectives and the longer term big picture. Acting within adversaries' decision cycles is also key because tempo and adaptability count. Frequently there will be a limited window of opportunity for specific messages to achieve a desired result.

An organization must remain flexible enough to address specific issues with specific audiences, often at specific moments in time, by communicating to achieve the greatest effect. All communication carries inherent risk and requires a level of risk acceptance within the organization. Leaders must develop and instill a culture that rewards initiative while not overreacting to setbacks and miscues. While risk must be addressed in the form of assumptions in planning, it should not restrain leaders' freedom of action providing it has been taken into consideration appropriately.

Continuous. Diligent ongoing research, analysis, planning, execution, and assessment that feeds planning and action.
Strategic Communication is a continuous process of research and analysis, planning, execution, and assessment. Success in this process requires diligent and continual analysis and assessment feeding back into planning and action. Strategic Communication supports the organization's objectives by adapting as needed and as plans change. The SC process should ideally operate at a faster tempo or rhythm than our adversaries.

Under Secretary of State for Public Diplomacy and Public Affairs -- U.S. Department of State

The Under Secretary of State for Public Diplomacy and Public Affairs, Judith A. McHale, is responsible for U.S. global engagement and the Department of State's engagement with foreign and American publics. These functions are indispensable to the conduct of foreign policy. The focus of the Under Secretary's effort is in three areas:

1. leading the U.S. government effort in the global strategic communication,
2. building on the strengths of U.S. educational and cultural exchanges, and
3. bringing fresh and vital technologies to bear on all of our efforts.

The Under Secretary supervises directly three major bureaus (International Information Programs, Public Affairs, Educational and Cultural Affairs). Because her office manages special appropriations and programs, it includes an Office of Policy, Planning and Resources. Additionally, the importance of the private sector in contributing to public diplomacy efforts has been recognized by the establishment of the Office of Private Sector Outreach. Field operations are carried out by over 1000 public diplomacy officers based in over 200 embassies, consulates and other missions abroad. The Under Secretary also is the Administration's voting representative on the Broadcasting Board of Governors, the executive agency that directs American civilian international broadcasting (Voice of America, RFE/RL, Radio Marti, Radio Sawa, Al Hurra and other radio and television programming aimed at foreign audiences).

1. Office of Policy, Planning and Resources for Public Diplomacy and Public Affairs (R/PPR). Created in September 2004 to provide long-term strategic planning and performance measurement capability for public diplomacy and public affairs programs, this office assists the Under Secretary on allocation of public diplomacy and public affairs resources, focuses these on the priority national security objectives, and developes public diplomacy strategy documents.

2. Global Strategic Engagement Center (GSEC): Created originally as the Counter Terrorism Communication Center, this office now serves both the Under Secretary and the NSC-led Interagency Policy Committee on Global Engagement and Strategic Communication. GSEC integrates, coordinates, and de-conflicts department and agency global engagement and strategic communication. GSEC coordinates the Department's public diplomacy presence in the interagency, in consultation with other State bureaus.

3. Office of Private Sector Outreach (R/PSO). The Office of Private Sector Outreach works to develop and coordinate innovative ways for the State Department to engage the private sector in public diplomacy initiatives. The department recognizes that the work of public diplomacy is certainly not the work of government alone. The Office therefore works to engage America's private sector leaders in dynamic partnerships to empower women business leaders, provide much needed humanitarian relief, strengthen international education, encourage health advocacy, and promote social and economic development throughout the world.

4. The Bureau of Educational and Cultural Affairs (ECA) fosters mutual understanding between the people of the United States and other countries. It does this in close cooperation with State Department posts through education, cultural and professional exchanges as well as presenting U.S. history, society, art, and culture in all of its diversity to overseas audiences. The bureau manages the prestigious Fulbright Scholars program as well as the International Visitor Program, high school exchanges, English teaching, many work-study exchanges and university-to-university linkages. ECA awards millions of dollars in grants to American organizations for specific initiatives, while public diplomacy officers in the field have authority to grant monies to host nation persons, institutions and NGO's in support of mission strategic goals.

5. Bureau of International Information Programs (IIP) The principal international strategic communication entity for the foreign affairs community, IIP informs, engages, and influences international audiences (but not U.S. domestic audiences) about U.S. policy and society in order to advance America's interests. IIP develops and implements public diplomacy strategies to influence international audiences through information programs, foreign language websites (see http://www.america.gov), publications, and new technologies. It is prohibited from disseminating its products to the domestic audience by the Smith-Mundt Act, and amendments. The Congress has approved having an Assistant Secretary lead this bureau, an indication of its increasingly important role in the current struggle against violent extremism.

6. Bureau of Public Affairs. This bureau helps Americans understand U.S. foreign policy and the importance of foreign affairs by responding to press inquiries, holding press briefings; hosting "town meetings" and other conferences around the U.S. and arranging local, regional, and national radio and television interviews with key Department officials; and providing audio-visual products and services. The bureau provides additional information and services by maintaining the State Department website at http://www.state.gov and a telephone information line (202-647-6575) for public inquiries. In addition, the Office of the Historian provides historical research and advice for the Department of State and publishes the official documentary history of U.S. foreign policy. The Bureau is led an Assistant Secretary, and includes the office of the Department's spokesman.

Website: http://usinfo.state.gov and http://www.state.gov/r/
Last Updated: 14 October, 2009

National Strategy and Agencies

Included in this section are descriptions of the U.S. National Strategy for Public Diplomacy and Strategic Communication & the National Security Agency

U.S National Strategy for Public Diplomacy and Strategic Communication

The National Strategy for Public Diplomacy and Strategic Communication was published 31 May 2007. It is unclear at the time of this writing whether this document has been adopted by the Obama administration. It is, however the latest national security document on this topic and so is provided in that light. The complete document is at:

http://www.carlisle.army.mil/DIME/documents/National%20Strategic%20Communications%20Plan%20w%20kph%20changes.pdf

The strategy focuses on three key strategic objectives that govern America's communication with foreign audiences: The United States should offer a positive vision of hope and opportunity to the world; isolate and marginalize violent extremists and; nurture common interests and values between Americans and foreign publics.

In addition to the three strategic objectives above the strategy aims to support achievement of the National Security Strategy Objectives. Public diplomacy and strategic communication should always strive to support our nation's fundamental values. All communication and public diplomacy should (1) underscore our commitment to freedom, human rights and the dignity and equality of every human;, (2) reach out to those who share our ideals; (3) support those who struggle for freedom and democracy; and (4) counter those who espouse ideologies of hate and oppression.

Strategic audiences are (1) Key Influencers **--** those whose views can have a ripple effect throughout society. They include clerics, educators, journalists, women leaders, business and labor leaders, political leaders, scientists and military personnel. (2) Vulnerable Populations **--** those groups most vulnerable to extremist ideology, like youth and women and girls as well as minorities. (3) Mass Audiences – the United States must expand its presence on international broadcasts and rapidly develop improved capabilities to employ the power of Internet and other new technologies.

Public diplomacy priorities are programs and activities that expand education and exchange programs, modernize communications, and promote the "diplomacy of deeds". Under the Bush II administration the Policy Coordinating Committee (PCC) on Public Diplomacy and Strategic Communication led by the Under Secretary for Public Diplomacy and Public Affairs was the overall mechanism to coordinate our public diplomacy across the interagency community. (Note: the Obama administration has established an Interagency Policy Committee on Global Engagement and Strategic Communication, led by NSC that effectively replaces this PCC). To accomplish this, the PCC established the following structures: (1) Counterterrorism Communications Center headquartered at the Department of State, with the core mission of developing messages and strategies to discredit terrorists and their ideology; (2) the Interagency Crisis Communication Team **--** the National Security Council will initiate an interagency conference call immediately upon major breaking news that might have an impact on our efforts against violent extremism to coordinate message points; (3) Regular Monitoring of Implementation of the strategy.

The strategy directs that each agency and embassy should develop its own specific plan to implement the objectives of the document. It also gives guidance that each agency's plan should identify two or three key programs/policies which the agency will highlight to support the overall public diplomacy/strategic communication goals, identify target audiences, assign responsibility and outline specific plans for communicating key programs, and policies to the target audiences through speeches, foreign travel, media interviews, etc.. Additionally, each agency must identify NGO and private sector partners with whom the agency works, subject matter experts who can explain and advocate U.S. policy, and workers who speak foreign languages and could translate/participate in interviews. Each agency must also recommend envoys to advance public diplomacy efforts, outline current activities and programs that can be linked to support global public diplomacy, and develop criteria to evaluate effectiveness.

The strategy recognizes the importance of basic information sharing. To support this, the State Department created a new "Public Diplomacy Briefing Book" that is available via the internet to update all USG officials on regional and country-specific policies, official statements and key messages, compelling stories, provide a database of images and videos, and information that represents mainstream Muslim views and rejection of terrorist/extremism. Additionally, best practices will be identified and shared through agency websites.

Further it recognized the importance of audience analysis: Understanding foreign public opinion is vital to successful communication. The USG should create a central repository of information and analysis of public opinion in different countries so we can better understand how citizens of other countries view us and what values and interests we have in common.

Proactive media booking is directed. The State Department's regional media hubs in London, Brussels and Dubai are equipped to support messaging and booking of senior USG officials abroad to project American viewpoints.

CONCLUSION

Public diplomacy is, at its core, about making America's diplomacy public and communicating America's views, values and policies in effective ways to audiences across the world. Public diplomacy promotes linkages between the American people and the rest of the world by reminding diverse populations of our common interests and values. Some of America's most effective public diplomacy is communicated not through words but through our deeds, as we invest in people through education, health care and the opportunity for greater economic and political participation. Public diplomacy also seeks to isolate and marginalize extremists and their ideology. In all these ways, public diplomacy is "waging peace," working to bring about conditions that lead to a better life for people across the world and make it more difficult for extremism to take root.

There are five attachments to the plan:

Attachment A: ACTION PLAN FOR STRATEGIC OBJECTIVES

Attachment B: GENERAL COMMUNICATION GUIDELINES.

Attachment C: CORE MESSAGES

Attachment D: ADDITIONAL COMMUNICATION VEHICLES.

Attachment E: EVALUATION AND ACCOUNTABILITY.

Updated: October 2009

National Security Agency (NSA)

National Security Agency/Central Security Service (NSA/CSS)

Introduction

The ability to understand the secret communications of our adversaries while protecting our own communications – a capability in which the United States (U.S.) leads the world – gives our nation a unique advantage.

Executive Order No. 12333, dated December 4, 1981, as recently amended (July 2008) describes the responsibilities of the NSA/CSS in more detail. The resources of the NSA/CSS are organized for the accomplishment of two national missions:

The Signals Intelligence (SIGINT) mission allows for an effective, unified organization and control of all foreign signals collection and processing activities of the U.S. The NSA/CSS is authorized to produce SIGINT in accordance with the objectives and priorities established by the Director of National Intelligence in consultation with the President's Foreign Intelligence Advisory Board. Foreign signals collection is a Title 50 United States Code (USC) authority given to the Director, NSA/CSS.

The Information Assurance (IA) mission provides the IA and Computer Network Defense (CND) solutions/services, and conducts Defensive Information Operations (DIO) in order to protect information processed by U.S. national security systems. The intent is to measurably improve the security of critical operations and information by providing know-how and technology to our suppliers, partners and clients, when and where they need them. The NSA/CSS's IA mission is authorized by National Security Directive 42.

The NSA/CSS is America's cryptologic organization. It produces foreign signals intelligence and performs highly specialized activities to protect U.S. Government national security information systems. A high technology organization, the NSA/CSS is on the frontiers of communications and data processing. It is also one of the most important centers of foreign language analysis and research within the U.S. Government. It is said to be the largest employer of mathematicians in the U.S. and perhaps the world. Its mathematicians design cipher systems that search for weaknesses in adversaries' systems/codes and that protect the integrity of U.S. systems.

SIGINT is a unique discipline with a long and storied past. Its modern era dates to World War II, when the U.S. broke the Japanese military code and learned of plans to invade Midway Island. This intelligence allowed the U.S. to defeat Japan's superior fleet. The use of SIGINT is believed to have directly contributed to shortening the war by at least one year. Today, SIGINT continues to play an important role in keeping the United States a step ahead of its enemies.

The IA mission becomes increasingly more challenging as the world becomes more technology-oriented. IA professionals go to great lengths to make certain that Government systems remain impenetrable. The NSA/CSS supports the highest levels of the U.S. Government to the war fighter.

The NSA/CSS conducts one of the U.S. Government's leading Research and Development (R&D) programs. Some of the Agency's R&D projects have significantly advanced the state of the art in the scientific and business worlds. The NSA/CSS's early interest in cryptanalytic research led to the first large-scale computer and the first solid-state computer, predecessors to modern computing. The NSA/CSS also made ground-breaking developments in semiconductor technology and remains a world leader in many technological fields.

Technology and the world change rapidly, and great emphasis is placed on staying ahead of these changes with employee training programs. The National Cryptologic School is indicative of the Agency's commitment to professional development. The school not only provides unique training for the NSA workforce, but it also serves as a training resource for the entire Department of Defense (DoD). The NSA/CSS sponsors employees for bachelor and graduate studies at the Nation's top universities and colleges, and selected Agency employees attend the various war colleges of the U.S. Armed Forces.

Most NSA/CSS employees, both civilian and military, are headquartered at Fort Meade, Maryland, centrally located between Baltimore, MD and Washington, D.C. Its workforce represents an unusual combination of specialties: analysts, engineers, physicists, mathematicians, linguists, computer scientists, researchers, as well as customer relations specialists, security officers, data flow experts, managers, administrative officers and clerical assistants.

SIGINT Mission

The NSA/CSS collects, processes and disseminates foreign SIGINT. The old adage that "knowledge is power" has perhaps never been truer than when applied to today's threats against our nation and the role SIGINT plays in overcoming them.

The NSA/CSS's SIGINT mission protects the nation by: Providing information in the form of SIGINT products and services that enable our government to make critical decisions and operate successfully; Protecting the rights of U.S. citizens by adhering to the provisions of the 4th amendment to the Constitution and; Using the nation's resources responsibly, according to the best management processes available.

Other Intelligence Community (IC) agencies are responsible for other types of intelligence: Central Intelligence Agency (CIA) - Human Intelligence (HUMINT); Defense Intelligence Agency – HUMINT and Measurement and Signature Intelligence (MASINT) and; National Geospatial Agency (NGA) – Imagery Intelligence

These different yet complementary disciplines give our nation's leaders a greater understanding of the intentions of our enemies.

The NSA/CSS's SIGINT mission provides our military leaders and policy makers with intelligence to ensure our national defense and to advance U.S. global interests. This information is specifically limited to that on foreign powers, organizations or persons and international terrorists. The NSA/CSS responds to requirements levied by intelligence customers, which includes all departments and levels of the U.S. Executive Branch of Government.

The prosecution of the SIGINT mission has evolved from the relatively static, industrial age, Cold War communications environment to the ubiquitous, high speed, multi-functional technologies of today's information age. The ever-increasing volume, velocity and variety of today's communications make the production of relevant and timely intelligence for military commanders and national policy makers more challenging than ever.

As much as modern telecommunications technology poses significant challenges to SIGINT, the many languages used in the nations and regions of the world that are of interest to our military and national leaders require the NSA/CSS to maintain a wide variety of language capabilities. Successful SIGINT depends on the skills of not only language professionals but those of mathematicians, analysts, and engineers, as well. The nation is indebted to them for the successes they have won.

IA Mission

IA is one of the two core missions of the NSA/CSS. The Information Assurance Directorate (IAD) is dedicated to providing IA solutions that will keep U.S. national security systems safe from harm.

IA refers to the measures intended to protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

The IAD’s mission involves detecting, reporting, and responding to cyber threats; making encryption codes to securely pass information between systems; and embedding IA measures directly into the emerging DoD’s Global Information Grid (GIG). It includes building secure audio and video communications equipment, making tamper protection products, and providing trusted microelectronics solutions. It entails testing the security of customers’ systems, providing Operations Security (OPSEC) assistance, and evaluating commercial software and hardware against nationally set standards to better meet our nation’s needs.

The IAD’s mission has evolved through three very distinct stages: Communications Security (COMSEC), Information Systems Security (INFOSEC), and IA. Following World War II and the Korean War, efforts focused primarily on cryptography (i.e. designing and building encryption devices to provide confidentiality for information). COMSEC is defined as the measures taken to deny unauthorized persons information derived from telecommunications and to ensure the authenticity of such telecommunications. COMSEC includes cryptographic security, transmission security, emission security, and physical security of COMSEC material.

In the 1980s, the introduction and widespread use of computers created new demands to protect information exchanges between interconnected computer systems. This demand created the Computer Security (COMPUSEC) discipline. However, the community recognized that stand-alone COMSEC and COMPUSEC activities could not protect information during storage, processing or transfer between systems. This recognition gave rise to the term INFOSEC and the information protection mission took on a broader perspective. INFOSEC is defined as the protection of information systems against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users, including those measures necessary to detect, document, and counter such threats.

In the 1990s, IA emerged and focused on the need to protect information during transit, processing, or storage within complex and/or widely dispersed computers and communication system networks. IA also includes a dynamic dimension where the network architecture is itself a changing environment, including the information protection mechanisms and features that detect attacks and enable a response to those attacks. IA measures protect against the exploitation or penetration efforts routinely conducted by sophisticated adversaries, but also protect against hackers or criminals from creating havoc across layered domains.

Today, IA incorporates more than just the need for confidentiality achieved through the use of encryption products that the NSA/CSS produces or certifies. IA also includes the DIO elements that protect and defend information and information systems.

Contact Information: Community Outreach Office (410) 854-0903

Website: http://www.nsa.gov/

Updated: October 2009

Department of Defense Directives and Roadmaps

Included in this section are the *DoD Directive (DoDD) 3600.01* and the *2006 Quadrennial Defense Review (QDR) Execution Roadmap for Strategic Communication*.

Department of Defense Directive (DoDD) 3600.01 Information Operations

This section presents a synopsis of non-restricted information from the current Department of Defense Directive.

Purpose. Department of Defense Directive (DoDD) 3600.01, “Information Operations” is the *fundamental* document for both understanding and employing Information Operations (IO). As such it should be the starting point for all study of Information Operations as undertaken by U.S. practitioners. It gives policy guidance to the Department of Defense for the management and implementation of IO throughout DoD, sets out responsibilities for the key offices at OSD and joint command levels and gives definitions to key terms.

Scope. As policy guidance, it defines terms; assigns responsibilities to officials, services, unified commands, and agencies; and provides the basis for the development of joint and service doctrine for IO. The term, “doctrine”, as defined by Joint Publication 1-02, "DoD Dictionary of Military and Associated Terms” (October, 2004) means: “*Fundamental principles by which the military forces or elements thereof guide their actions in support of national objectives. It is authoritative but requires judgment in application”*.

Information Operations (IO) Defined. IO is “The integrated employment of the core capabilities of Electronic Warfare (EW), Computer Network Operations (CNO), Psychological Operations (PSYOP), Military Deception (MILDEC), and Operations Security (OPSEC), in concert with specified supporting and related capabilities, to influence, disrupt, corrupt, or usurp adversarial human and automated decision-making while protecting our own”.

Use of IO. IO is to be employed to support full spectrum dominance by taking advantage of information technology, maintaining U.S. strategic dominance in network technologies, and capitalizing upon near real-time global dissemination of information, to affect adversary decision cycles with the goal of achieving information superiority for the United States.

Core IO Capabilities.

IO employs five core capabilities to achieve desired Combatant Commander effects or prevent the enemy from achieving his desired effects: ***EW, CNO, PSYOP, MILDEC, and OPSEC***. They are operational in a direct and immediate sense; they either achieve critical operational effects or prevent the adversary from doing so. They are interdependent and increasingly need to be integrated to achieve desired effects.

Supporting Capabilities (See Glossary for definitions):

- Counterintelligence
- Physical (kinetic) attack
- Physical Security
- Information Assurance (IA)
- Combat Camera

Related Capabilities. (See Glossary for definitions):

- Public Affairs (PA)
- Civil-Military Operations (CMO)
- Defense Support to Public Diplomacy (DSPD)

Intelligence Support. Intelligence will be developed, consistent with the National Intelligence Priorities Framework, to provide data about adversary information systems or networks; produce political-military assessments; conduct human factors analysis; and provide indications and warning of adversary IO, including threat assessments.

RESPONSIBILITIES. The following officials, commands, and agencies are tasked with the specific responsibilities indicated:

<u>Under Secretary of Defense for Intelligence (USD(I))</u> :

- Serve as the Principal Staff Assistant to the Secretary of Defense for IO.
- Develop and oversee DoD IO policy and integration activities.
- Assess performance/responsiveness of DoD and Military Intelligence activities to support IO.
- Coordinate, oversee, and assess the efforts of the DoD Components to plan, program, develop, and execute capabilities in support of IO requirements.
- Establish specific policies for the development and integration of CNO, MILDEC and OPSEC as core IO capabilities.

<u>Under Secretary of Defense for Acquisition, Technology and Logistics (USD(AT&L))</u> :

- Establish specific policies for the development and integration of EW as a core IO capability.
- Develop and maintain a technology investment strategy for development, acquisition, and integration of EW capabilities.
- Invest in and develop the science and technologies needed to support IO capabilities.

<u>The Under Secretary of Defense for Policy (USD(P))</u>:

- Provide DoD oversight of IO planning, execution, and related policy guidance including the establishment of an OSD review process to assess IO plans and programs
- Lead interagency coordination, exclusive of the IC, and international cooperation involving planning and employment of IO capabilities.
- Establish specific policy and oversight for development and integration of PSYOP as a core IO capability and DSPD as a related capability.

<u>The Under Secretary of Defense for Personnel and Readiness (USD(P&R))</u>:

- Develop policy and procedures on matters pertaining to the establishment and management of an IO career force in coordination with the Secretaries of the Military Departments, the Chairman of the Joint Chiefs of Staff, the USD(P), the USD(I), and others, as appropriate.
- Provide training policy and oversight as it pertains to the integration of all IO capabilities into joint exercises and joint training regimes.

The Assistant Secretary of Defense for Networks and Information Integration/ DoD Chief Information Officer (ASD(NII)/DoD CIO) will:

- Establish specific policy for the development and integration of IA and Computer Network Defense (CND) as related to CNO as a core IO capability.
- Oversee and assess the efforts of the Heads of the DoD Components to plan, program, develop, and field IA and CND capabilities in support of CNO.

Assistant Secretary of Defense for Public Affairs will:

- Establish specific policy for the relationship of PA to IO.
- Oversee PA planning and coordination efforts as related to IO within DoD
- Oversee the development and conduct of appropriate training and education that defines PA's relationship to IO for public affairs and visual information personnel at the Defense Information School.

Commander, U.S. Strategic Command (CDRUSSTRATCOM):

- Integrate and coordinate DoD IO core capabilities that cross geographic areas of responsibility or core IO areas.

Commander, U.S. Special Operations Command (CDRUSSOCOM)

- Integrate and coordinate DoD PSYOP capabilities to enhance interoperability and support USSTRATCOM's information operations responsibilities and other combatant commanders' PSYOP planning and execution.
- Support the other Combatant Commanders though joint employment of PSYOP and other special operations force IO capabilities.
- Employ other special operations force IO capabilities as directed.

The Secretaries of the Military Departments and CDRUSSOCOM:

- Develop IO doctrine and tactics, and organize, train, and equip for IO for their Title 10 (U.S. Code) and Major Force Program responsibilities.

The Chairman of the Joint Chiefs of Staff

- Serve as the principal military advisor to the President of the United States, the National Security Council, and the Secretary of Defense on IO.
- Validate capability-based IO requirements through the Joint Requirements Oversight Council.
- Develop and maintain joint doctrine for core, supporting, and related IO capabilities in joint operations.
- Ensure all joint education, training, plans, and operations include, and are consistent with, IO policy, strategy, and doctrine.

Definitions. See Glossary for definitions of the following terms: Computer Network Attack, Computer Network Defense, Computer Network Exploitation, Computer Network Operations, Defense Support to Public Diplomacy, Electronic Warfare, Human Factors, Information, Information Assurance, Information Operations Specialists and Planners, Information Superiority, Information System, Military deception, Operations Security, Psychological Operations, Public Affairs, and Public Diplomacy.

DoDD 3600.01 can be viewed at:
http://www.dtic.mil/whs/directives/search.html and enter 3600.01

Last Reviewed October 2009

QDR Execution Roadmap for Strategic Communication

This section provides a synopsis of the 2006 Quadrennial Defense Review (QDR) Execution Roadmap for Strategic Communication

The QDR Execution Roadmap for Strategic Communication was signed by Deputy Secretary of Defense Gordon England on 25 September 2006. The complete roadmap can be found at http://www.carlisle.army.mil/DIME/documents/QDR%20SC%20Roadmap%20final.pdf. The QDR Roadmap is no longer being monitored for milestone execution, but it remains the most current official DoD publication on this topic and is provided in that light.

Purpose: The purpose of the QDR Execution Roadmap is to provide guidance for implementing Strategic Communication direction for the 2006 Quadrennial Defense Review (QDR). It includes a plan of action and milestones (POA&AM) which assigns objectives tasks, and milestones, with associated offices of Primary Responsibility (OPR). The roadmap also provides an initial estimate of the costs of improving capabilities that support Strategic Communication and provides senior leadership with a mechanism to advance high priority issues for decision through the Fiscal Years (FY) 2008-2013. The Roadmap identified important actions and leads for each of 55 tasks identified. Approximately 35 tasks that were to be completed within a year of the publication of the Roadmap

Statement of the Problem: The Roadmap stated that the problem was that the U.S. military is not sufficiently organized, trained or equipped to analyze, plan, coordinate and integrate the full spectrum of capabilities available to promote America's interests as part of a national effort to improve the integration of information as a vital element of national power. The current changes in the global information environment require the Department of Defense (DoD), in conjunction with other U. S. Government (USG) agencies, to implement more deliberate and well-developed strategic communication processes.

Definition of Strategic Communication: The Roadmap defined Strategic Communication as: "Focused United States Government processes and efforts to understand and engage key audiences to create, strengthen, or preserve conditions favorable to advance national interests and objectives through the use of coordinated information, themes, plans, programs, and actions synchronized with other elements of national power."

Goal: DoD will increase its effectiveness in strategic communication by developing a culture that recognizes the value of communication and integrates communication considerations into policy development, operational planning, execution, and assessment to advance national interests.

Objectives. The Roadmap defined three objectives for achieving DoD's goal of effective strategic communication:

Objective 1. Institutionalize a DoD process by which principles of strategic communication are incorporated in the development of strategy, policy formulation, planning, and execution.

Two major tasks identified in support of institutionalizing the DoD process include facilitating horizontal integration of strategic communication within DoD and improving the integration of the DoD's strategic communication process with the strategic communication process of the U.S. Government.

To help the internal DoD integration the Roadmap directed the establishment of DoD Strategic Communication Integration Group (SCIG) that will provide recommendations to integrate strategic communication throughout OSD, the Joint Staff, Combatant Commands, Military departments and other elements of DoD. Further, it directed the creation of a DoD Strategic Communication Secretariat staffed with personnel from OSD, Joint Staff, and included Military Department Liaisons, to support the DoD SCIG. (Note that these organizations were disbanded after an initial pilot period and subsequent review).

To improve the integration with the U.S. Government strategic communication process the Roadmap directed the Undersecretary of Defense for Policy (USD(P)), in coordination with the Assistant Secretary of Defense for Public Affairs to begin conferences within DoD and follow on conferences with Department of State (DOS) and to develop a formal process to coordinate and synchronize DoD strategic communication activities with key allies and coalition partners.

Objective 2. Define roles, responsibilities and relationships, and develop doctrine for strategic communication and its primary communication supporting capabilities: Public Affairs (PA); aspects of Information Operations (IO), principally PSYOP; Visual Information (VI) and the DoD activities of Military Diplomacy (MD), and Defense Support to Public Diplomacy (DSPD). To accomplish this objective, the Roadmap directed the development of DoD Directive on strategic communication and on military diplomacy, and Chairman Joint Chief of Staff Instructions on defense support to public diplomacy plus a review of other DoD Directives, Instructions and Publications for strategic communication implications.

Objective 3. Properly resource Military Departments and Combatant Commands to organize, train, and equip DoD's primary communication supporting capabilities. In order to accomplish this objective, the Roadmap described tasks to be accomplished to include the development of concept of operations (CONOPS) for the Joint Public Affairs Support Element (JPASE), Joint Psychological Operations Support Element (JPSE), as well as a CONOPS for VI. Additional tasks were identified along with projected FY 08 and future FY impact in dollar amounts needed to accomplish the task.

Last Updated: October 2009

Department of Defense Organizations

Included in this sections descriptions of the following organizations:

Under Secretary Of Defense – Policy (USD(P))

Under Secretary of Defense for Intelligence (USD(I))

Assistant Secretary of Defense – Networks and Information Integration (ASD(NII))

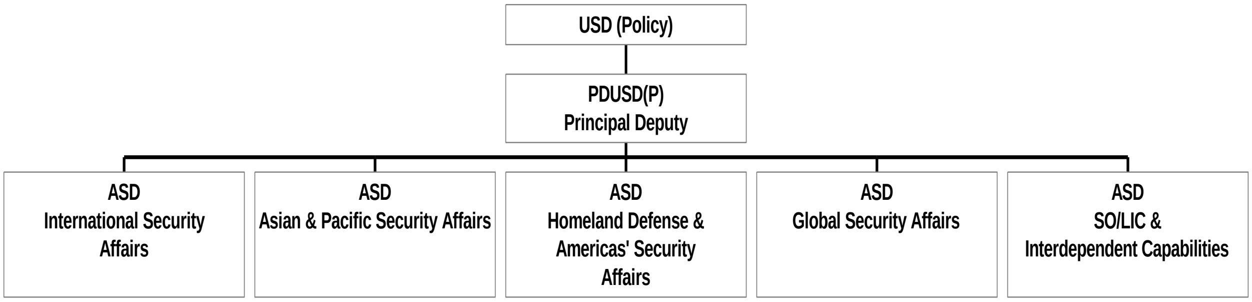
Defense Information Systems Agency (DISA)

Information Assurance Technology Analysis Center (IATAC)

This Page Intentionally Blank

Under Secretary Of Defense – Policy (USD(P))

Mission: The mission of the Office of the Under Secretary of Defense for Policy is to consistently provide responsive, forward-thinking, and insightful policy advice and support to the Secretary of Defense, and the Department of Defense, in alignment with national security objectives.


USD (Policy)
PDUSD(P)
Principal Deputy
ASD
International Security Affairs
ASD
Asian & Pacific Security Affairs
ASD
Homeland Defense & Americas' Security Affairs
ASD
Global Security Affairs
ASD
SO/LIC & Interdependent Capabilities

The directed responsibilities of the USD(P) include but are not limited to the following:

- Represent the Department of Defense, as directed, in matters involving the National Security Council (NSC); the Department of State; and the other Federal Departments, Agencies, and inter-Agency groups with responsibility for national security policy.

- Serve as a member of the NSC Deputies Committee; serve as a member of the Deputies Committee for Crisis Management; and advise the Secretary of Defense on crisis prevention and management, including contingency planning for major areas of concern.

- Develop DoD policy guidance, provide overall supervision, and provide oversight of planning, programming, budgeting, and execution of special operations activities, including civil affairs and psychological operations, and of low-intensity conflict activities, including counter-terrorism, support to insurgency, and contingency operations.

- Develop policy and provide oversight for emergency planning and preparedness, crisis management, defense mobilization in emergency situations, military support to civil authorities, civil defense, and continuity of operations and government. Develop policy and coordinate DoD participation in, and exercise staff supervision over, special activities, special access programs, sensitive support to non-DoD agencies, and the joint worldwide reconnaissance schedule.

Principal Deputy Undersecretary of Defense for Policy – PDUSD(P)-- Provides advice and assistance to the Secretary of Defense, Deputy Secretary of Defense and the Under Secretary of Defense for Policy on national security policy, military strategy, and defense policy.

The Assistant Secretary of Defense for International Security Affairs – The Assistant Secretary of Defense for International Security Affairs is the principal advisor to the Under Secretary of Defense for Policy (USD(P)) and the Secretary of Defense on international security strategy and policy on issues of DoD interest that relate to the nations and international organizations of Europe (including the North Atlantic Treaty Organization), the Middle East, and Africa, their governments and defense establishments; and for oversight of security cooperation programs and foreign military sales programs in these regions.

The Assistant Secretary of Defense for Asian and Pacific Security Affairs - The office of Asian and Pacific Affairs Security Affairs is responsible for U.S. security and defense policy in the Asia-Pacific region.

The Assistant Secretary of Defense for Homeland Defense & Americas' Security Affairs – the following offices fall under the ASD for Homeland Defense and Americas' Security Affairs:

- Office of the Deputy Assistant Secretary of Defense for Homeland Defense & Defense Support to Civil Authorities (DSCA)
- Office of the Deputy Assistant Secretary of Defense for Western Hemisphere Affairs
- Office of Deputy Assistant Secretary of Defense for Crisis Management & Mission Assurance

The responsibilities of the ASD for Homeland Defense & Americas Security Affairs are best described by going to the web page:
http://policy.defense.gov/sections/policy_offices/hd/index.html

The Assistant Secretary of Defense for Global Strategic Affairs – the following offices and responsibilities fall under the ASD for Global Strategic Affairs:

- Office of the Deputy Assistant Secretary of Defense for Countering-WMD
- Office of the Deputy Assistant Secretary of Defense for Nuclear & Missile Defense Policy
- Office of the Deputy Assistant Secretary of Defense for Cyber & Space Policy

The Assistant Secretary of Defense for Special Operations/Low Intensity Conflict and Interdependent Capabilities. The Assistant Secretary of Defense for Special Operations/Low-Intensity Conflict and Interdependent Capabilities (ASD/SOLIC&IC) is the principal civilian advisor to the Secretary of Defense on special operations and low-intensity conflict matters. The ASD (SO/LIC&IC) has as his principal duty overall supervision (to include oversight of policy and resources) of special operations and low-intensity conflict activities. These core tasks, according to USSOCOM's 2007 Posture Statement, include counterterrorism; unconventional warfare; direct action; special reconnaissance; foreign internal defense; civil affairs, information and psychological operations; and counterproliferation of WMD. Section 167 of Title 10 USC provides a very similar but not identical list of SOF activities.

In addition to policy oversight for special operations and stability operations capabilities, the ASD (SO/LIC&IC) has policy oversight for strategic capabilities and force transformation and resources. This includes oversight of capability development to include general-purpose forces, space and information capabilities, nuclear and conventional strike capabilities, and missile defense. As such, ASD

(SO/LIC&IC), after the Secretary and Deputy Secretary, will be the principal official charged with oversight over all warfighting capabilities within the senior management of the Department of Defense.

The following offices fall under the ASD for Special Operations/Low Intensity Conflict and Interdependent Capabilities:

- Office of the Deputy Assistant Secretary of Defense for Special Operations Capabilities
- Office of the Deputy Assistant Secretary of Defense for Forces Transformation & Resources
- Office of the Deputy Assistant Secretary of Defense for Stability Operations Capabilities

Website: http://policy.defense.gov/

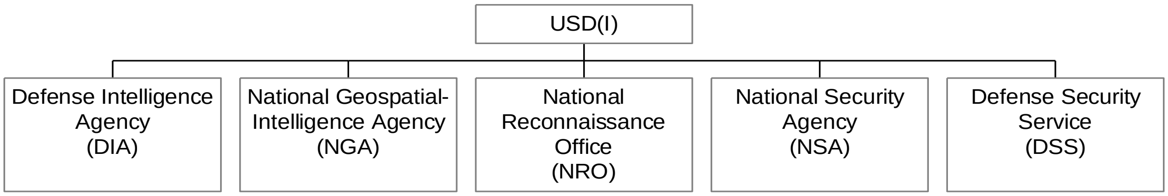
Last Updated: Nov 2009

This Page Intentionally Blank

Under Secretary Of Defense for Intelligence (USD(I))

Mission

The Under Secretary of Defense for Intelligence (USD(l)) serves as the Principal Staff Assistant (PSA) and advisor to the Secretary and Deputy Secretary of Defense on all intelligence, counterintelligence, security, sensitive activities, and other intelligence-related matters. The USD(I) also serves as the PSA to the Secretary of Defense on development and oversight of DoD IO policy and integration activities, and serves as the DoD lead with the Intelligence Community on DoD IO issues. Per a memorandum between the SecDef and the Director of National Intelligence (DNI) signed May 21, 2007, the USD(I) is also designated as the Director of Defense Intelligence (DDI) in the Office of the Director of National Intelligence. In this capacity, the USD(I) reports directly to the DNI and serves as the principal advisor to the DNI on defense intelligence matters.


USD(I)
Defense Intelligence Agency (DIA)
National Geospatial-Intelligence Agency (NGA)
National Reconnaissance Office (NRO)
National Security Agency (NSA)
Defense Security Service (DSS)

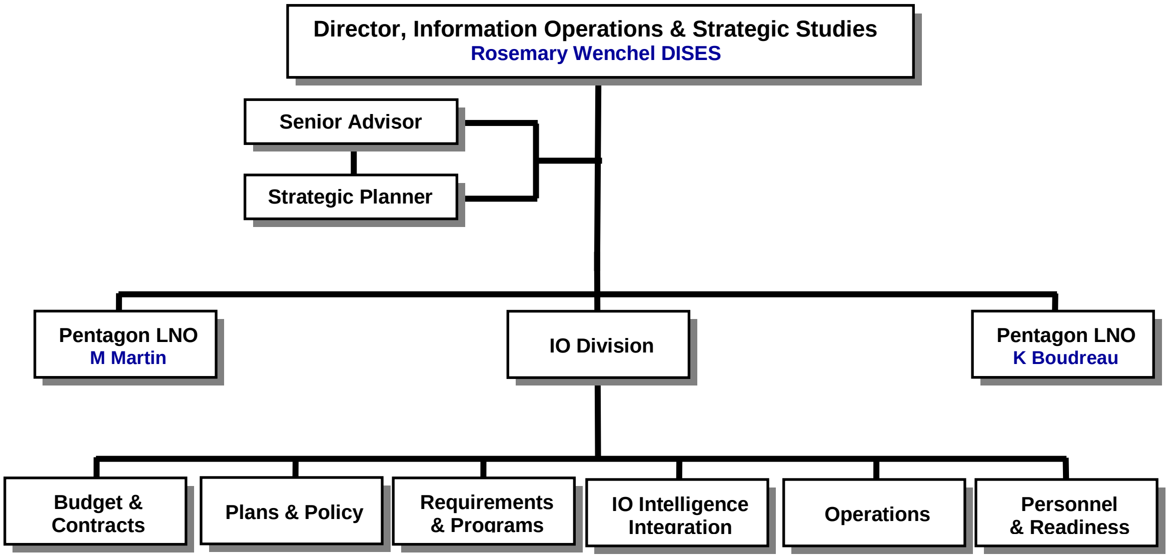
IO Responsibilities:

Information Operations Responsibilities:

- Serve as the Principal Staff Assistant to the Secretary of Defense for IO.
- Develop and oversee DoD IO policy and IO Intelligence Integration.
- Assess performance/responsiveness of DoD and Military Intelligence activities to support IO.
- Coordinate, oversee, and assess the efforts of the DoD Components to plan, program, develop, and execute capabilities in support of IO requirements.
- Establish specific policies for the development and integration of CNO, MILDEC and OPSEC as core IO capabilities.
- Serve as the OSD proponent for the Information Operations Career Force, per DoD I 3608.11, "Information Operations Career Force", 4 Nov 05.

OUSD(I) Organization

The Director of the Information Operations and Strategic Studies (DIOSS) reports to the Deputy Under Secretary of Defense for Joint and Coalition Warfighter Support. The IOSS Directorate supports the USD(I) IO PSA requirements, and is organized per the chart below



IO Issuances

The following OUSD(I) issuances are listed below:

- DoD Directive 5143.01, “Under Secretary of Defense for Intelligence (USD(I)),” November 23, 2005
- DoD Directive 3600.01, "Information Operations," August 14, 2006
- DoD Instruction O-3600.02, “Information Operations (IO) Security Classification Guidance,” November 28, 2005
- DoD Directive O-3600.03, “Technical Assurance Standard for Computer Network Attack Capabilities,” May 13, 2005
- DoD Instruction 3608.11, “Information Operations Career Force,” November 4, 2005
- DoD Instruction 3608.12, “Joint Information Operations Education,” November 4, 2005
- Under Secretary of Defense for Intelligence Memorandum, “Information Operations (IO) and Space Executive Committee (EXCOM) Charter,” January 11, 2005[1]

Last Updated: October 2009

Assistant Secretary Of Defense – Networks and Information Integration (ASD(NII))

Mission and Goals.

The missions and responsibilities of the ASD(NII) are specified in Department of Defense Directive (DoDD) 5144.1, "Assistant Secretary of Defense for Networks and Information Integration/ DoD Chief Information Officer (ASD(NII)/DoD CIO) " dated 2 May 2005.

The goals of ASD(NII) are to:

- Make information available on a network that people depend on and trust
- Populate the network with new, dynamic sources of information to defeat the enemy
- Deny the enemy information advantages and exploit weakness to support network centric warfare and the transformation of DoD business processes

Mission: The ASD(NII)/DoD CIO is the principal staff assistant and advisor to the Secretary of Defense and Deputy Secretary of Defense on networks and network-centric policies and concepts; command and control (C2); communications; non-intelligence space matters; enterprise-wide integration of DoD information matters; Information Technology (IT), including National Security Systems (NSS); information resources management (IRM); spectrum management; network operations; information systems; information assurance (IA); positioning, navigation, and timing (PNT) policy, including airspace and military-air-traffic control activities; sensitive information integration; contingency support and migration planning; and related matters.

ASD(NII)/DoD CIO has responsibilities for integrating information and related activities and services across the Department. The ASD (NII)/DoD CIO also serve as the DoD Enterprise-level strategist and business advisor from the information, IT, and IRM perspective.

Responsibilities of the ASD(NII)/DoD CIO include the following:

- Information Operations: Provide NII and CIO support to the mission of Information Operations IAW DoD Directive S-3600.1.
- Information Assurance: Develop and maintain the DoD Information Assurance (IA) program and associated policies, procedures, and standards required by DoD Directive S-3600.1, "Information Operations ".
- Transformation: Develop and implement network-centric policies, architectures, practices, and processes with emphasis on communications and information networks to enable Defense transformation; however, these do not include content-based communications functions such as those associated with public affairs and public diplomacy.

- Global Information Grid: Facilitate and resolve interoperability, performance, and other issues related to interfaces, security, standards, and protocols critical to the end-to-end operation of the Global Information Grid (GIG).
- IT Opportunities: Identify opportunities presented by communication and information technologies as well as risks and costs, and make recommendations on the initiation of communication and information plans, programs, policies, and procedures accordingly.
- Electromagnetic Spectrum: Provide policy, oversight, and guidance for all DoD matters related to the electromagnetic spectrum, including the management and use of the electromagnetic spectrum (MUES) and the Electromagnetic Environmental Effects (E3) Program.
- Command and Control: Develop and integrate the Department's overall C2 strategy, approach, structure, and policies and ensure the C2 structure and architecture are compliant with DoD network-centric precepts, information strategy, and joint needs.
- Space: Oversee DoD non-intelligence related space matters, including space-based communications programs, space-based information integration activities, space control activities, operationally responsive space programs, space access, satellite control, space-based position, navigation, and timing programs, environmental sensing, and space launch ranges.

Headquarters: The headquarters for the ASD(NII) organization is in the Pentagon, with staff elements both in the Pentagon and in nearby office buildings in Arlington, Virginia.

Website: http://www.defenselink.mil/nii/

Last Updated: October 2009

Defense Information Systems Agency (DISA)

Mission: DISA, a Combat Support Agency, engineers and provides command and control capabilities and enterprise infrastructure to continuously operate and assure a global net-centric enterprise in direct support to joint warfighters, National level leaders, and other mission and coalition partners across the full spectrum of operations. We are leaders enabling information dominance in defense of our Nation.

Operations and Activities:
DISA's current C2 programs include the Global Command and Control System - Joint (GCCS-J), Global Combat Support System - Joint (GCSS-J), and an Adaptive Planning and Execution (APEX) set of capabilities. Through ongoing efforts, DISA will evolve its current C2 programs to deliver a truly integrated, joint, net-centric C2 capability for the warfighter. DISA also has various Joint Capability Technology Demonstrations (JCTDs) that facilitate rapid development of advanced capabilities.

Through GCCS-J, DISA enables Joint operations planning and execution, global access to mandated readiness data, situational awareness via a common operational picture, Commander's understanding of the battlespace through imbedded/integrated intelligence and imagery products, and collaboration and decision support capabilities for Combatant Commanders and Joint Force Commanders. Deployed worldwide, GCCS-J components form the critical C2 backbone of Joint operations. Lighter, configurable deployments of GCCS-J support selected Joint Task Forces and Coalition operations. GCCS-J intelligence products and training are currently being used in direct support of OEF, OIF, and NATO/ISAF Afghanistan Operations. In addition, GCCS-J has successfully supported such non-traditional missions as investigation as a capability that could be used to deal with a potential Avian Flu pandemic. GCCS-J is in the midst of its version 4.2 fielding phase, which will provide even more substantial C2 capabilities to the Warfighter, including many technological solutions that exploit the emerging availability of the Service Oriented Architecture.

DISA provides the logistics C2 system of record through GCSS-J. GCSS-J is an integration and interoperability initiative to better meet the operational needs of the warfighter for combat support. As part of its mission, GCSS-J enhances combat support effectiveness through system interoperability across combat support and combat service support functions, and between combat support and command and control functions. GCSS CC/JTF expands the availability, accuracy, and timeliness of information to the combatant commanders and the joint task force commanders and their staffs through information fusion. End-users have the ability to create a user defined operational picture through dynamic access to disparate data sources and enhanced by a tool kit of capabilities such as knowledge management, business intelligence, watchboard, electronic battlebook, functional applications and access to other SIPRNet sites via one GCSS gateway.

Adaptive Planning and Execution (APEX) is the DoD's methodology for constructing timely and agile war plans that achieve national security objectives. At full maturity, the APEX system will be a collaborative planning and execution system that facilitates the rapid development and maintenance of plans and, when necessary, the dynamic transition to execution. The APEX system will address and provide combatant commands, Service/Functional Components, Combat Support Agencies (CSA) and the Joint Staff with an aligned end-to-end process, integrated with multi-national partners and US government departments and agencies as required, facilitated by trained personnel, and technology to support planning and execution.

Currently the Department of Defense has several disparate operational capabilities and systems that provide functionality to support the APEX business process. The DISA APEX PMO is responsible for providing adaptive planning and execution/force projection capabilities that will be accessible in a net-centric service oriented architecture environment and will focus on providing the joint forces commander with the data and information needed to make timely, effective, and informed decisions. The APEX strategy will provide new capabilities as well as evolve current disparate planning capabilities into a fully integrated, interoperable, and collaborative joint solution. The DISA APEX PMO is responsible for the development, integration, testing, and fielding of APEX enterprise capabilities for the Warfighter on the Global Information Grid (GIG).

DISA is deeply involved in JCTDs, working with the Combatant Commanders to pilot key capabilities essential to the Department's ongoing transformation. JCTDs respond to high-priority capability shortfalls involving complex conceptual or technical issues appropriately addressed early in a technology lifecycle. JCTDs are typically 18 months to three years in duration and are funded from multiple sources to include a percentage from the Director of Defense Research and Engineer’s Rapid Fielding office. JCTDs, are transitioned or made accessible to the user upon successful completion in one of five ways: Follow on Development, Production, Fielding, Sustainment; Certification & Accreditation; Industry &/or Community of Interest (COI) Development; Limited Operational Use (LOU) or Non-Materiel Follow-on Development & Publication. This gives Combatant Commanders yet another means of rapidly addressing immediate operational needs.

Over the last two years, DISA's active ACTDs and JCTDs include:

- Theater Effects-Based Operations (TEBO)
- Event Management Framework - EMF
- Coalition Secure Management and Operations Systems - COSMOS
- Joint Coordinated Real-time Engagement - JCRE
- Joint Force Projection - JFP
- Homeland Security/Defense C2 (HLS/D C2)
- Large Data
- Medical Situational Awareness In-Theater – MSAT
- Cross Domain Collaborative Information Environment (CDCIE
- Transnational Information Sharing Cooperation (TISC)
- National Senior Leadership Decision Support Service (NSLDSS)
- Actionable Situation Awareness Pull (ASAP)
- Tactical Service Provider (TSP)
- Agile Transportation 21st Century (AT21) & Turbo Planner

Website: http://www.disa.mil

Last Updated: November 2009

Information Assurance Technology Analysis Center (IATAC)

The Information Assurance Technology Analysis Center (IATAC) is a U.S. Department of Defense Information Analysis Center (IAC) sponsored by the Defense Technical Information Center (DTIC), a field operating agency under the Director, Defense Research & Engineering (DDR&E). [See internet site: http://www.dod.mil/ddre/.}

Mission:

Provide the DoD a central point of access for information on Information Assurance (IA) emerging technologies in system vulnerabilities, research and development, models, and analysis to support the development and implementation of effective defense against Information Warfare attacks.

Management and Direction of IATAC Operations:

IATAC operates under the direction of DTIC with technical assistance provided by a Government Steering Committee. The committee is made up of 19 Senior IA professionals from Government, Academia, and DoD and the research and development (R&D) community. They include representation from the Department of Homeland Security (DHS), Office of the Secretary of Defense's Defense Information Assurance Program (DIAP), U.S. Strategic Command (STRATCOM) and STRATCOM's Joint Task Force for Global Network Operations (JTF-GNO), National Security Agency (NSA), Naval Postgraduate School (NPS), OSD, and the Navy Information Operations Command - Norfolk, to name a few. The steering committee meets once a year and provides input and feedback to IATAC's operations, particularly the information management, collection, analysis, and dissemination efforts. Additionally, the Steering Committee recommends topics for our State-of-the-Art (SOAR) technical reports that IATAC researches and produces

History:

The United States is vulnerable to Information Warfare attacks because our economic, social, military, and commercial infrastructures rely on information systems and computing networks and they demand timely, accurate, and reliable information services. This vulnerability is complicated by the dependence of our DoD information systems on commercial or proprietary networks and the Internet which are readily accessed by both users and adversaries – from script kiddies to nation states and all the permutations in between. The identification of the critical paths and key vulnerabilities within the information infrastructure is an enormous task. Recent advances in information technology have made information systems easier to use, less expensive, and more available to a wide spectrum of potential adversaries.

The survivability, authenticity, and continuity of DoD information systems are of supreme importance to the nation - this includes other Federal Agencies, Military Services, Warfighters, and R&D community. With the increasing amount of concern and Information Warfare activities requiring rapid responses, it is difficult to ensure that all appropriate agencies and organizations have access to the knowledge and tools to protect from, react to, and defend against Information Warfare attacks. IATAC was established under the direction of DTIC and the integrated sponsorship by the Defense Information Systems Agency (DISA); the Office of the Assistant Secretary of Defense for Networks and Information Integration (ASD-NII)); the Joint Staff (J6); and DDR&E all tasked with the mission to develop IA policy.

Free Products and Services:

IATAC provides a central authoritative source for IA vulnerability data, information, methodologies, models, and analyses of emerging technologies relating to the survivability, authenticity, and continuity of operation of information systems critical to the nation's defense in support of the Warfighter's mission. IATAC's support extends across the spectrum from policy, doctrine, and strategy development, to R&D, S&T, engineering, and architecture, to operations and training. This spectrum of activities ensures the management, collection, analysis, and dissemination of a broad and growing library of scientific technical information (STI) related to IA. IATAC serves to help synchronize the IA community's efforts across that entire spectrum of activities integrating across government, academia, and industry.

Examples of the information that IATAC provides free of charge include: *Measuring Cyber Security and Information Assurance (IA)* SOAR; *Insider Threat* SOAR; a tools report database that contains information on a wide range of intrusion detection, vulnerability analysis, firewall applications, and anti-malware tools; a quarterly newsletter that provides timely IA articles; and an inquiry service to provide 4 hours of free IA research. All these products and more are available from the IATAC web site via a simple product request form or via subscription.

Additional IA information is available through DTIC via registration include: hundreds of thousands of scientific and technical documents across a wide spectrum from the Total Electronic Migration System (TEMS) (https://tems-iac.dtic.mil) and standard wiki collaboration and information from DoDTechipedia (https://www.dodtechipedia.mil/dodwiki).

IATAC operates as a specialized subject focal point, supplementing DTIC services within DoD Directive 3200.12, DoD Scientific and Technical Information Program (STIP), dated 15 February 1983.

Location and Contact Information:

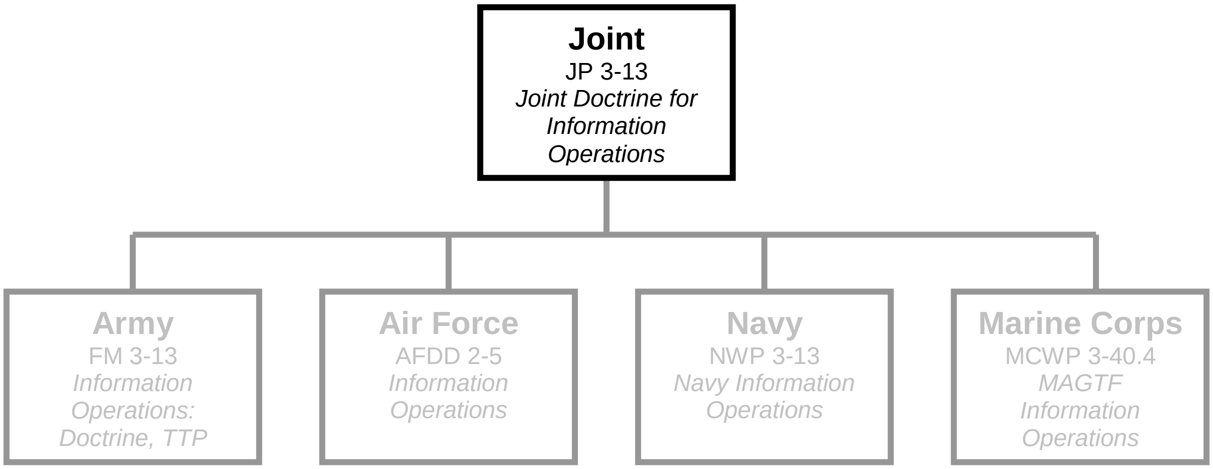
IATAC

13200 Woodland Park Road
Herndon, VA 20171
Phone: (703) 984.0775
Fax: (703) 984.0773
E-mail: iatac@dtic.mil

Website: iac.dtic.mil/iatac/

Last updated: October 2009

Joint Information Operations Doctrine



Joint
JP 3-13
Joint Doctrine for Information Operations

Army
FM 3-13
Information Operations: Doctrine, TTP

Air Force
AFDD 2-5
Information Operations

Navy
NWP 3-13
Navy Information Operations

Marine Corps
MCWP 3-40.4
MAGTF Information Operations

This Page Intentionally Blank

Joint Information Operations Doctrine

Key doctrinal documents:

Joint Pub 3-13, *Information Operations*, 13 February 2006
Joint Pub 3-13.1, *Electronic Warfare*, 25 January 2007
Joint Pub 3-13.3, *Operations Security*, 29 June 2006
Joint Pub 3-13.4, *Military Deception*, 13 July 2006
Joint Pub 3-53, *Doctrine for Joint Psychological Operations*, 5 September 2003
Joint Pub 3-57, *Joint Doctrine for Civil-Military Operations*, 08 July 2008
Joint Pub 3-61, *Public Affairs*, 9 May 2005

Joint Pubs available at: http://www.dtic.mil/doctrine/s_index.html and at
https://jdeis.js.mil/jdeis/index.jsp.

Joint Information Operations doctrine is set down in Joint Publication 3-13. This section extracts the publication's executive summary, below.

EXECUTIVE SUMMARY, JOINT PUBLICATION 3-13

- **Discusses the Information Environment and Its Relationship to Military Operations**
- **Discusses the Information Operations (IO) Core Capabilities Necessary to Successfully Plan and Execute IO to include Supporting and Related Capabilities in a Joint/Multinational Environment**
- **Aligns Joint IO Doctrine with the Transformational Planning Guidance as Specified by the Department of Defense IO Roadmap for Achieving Information Superiority on the Battlefield**
- **Provides an Organizational Framework for Integrating, Deconflicting, and Synchronizing IO Planning and Execution Activities for Supporting and Supported Combatant Command Staffs, National Intelligence Agencies, and Other Federal Agencies as Applicable**
- **Outlines Planning Considerations for Developing an IO Career Force through Joint Education, Training, Exercises, and Experimentation**

Military Operations and the Information Environment

To succeed, it is necessary for US forces to gain and maintain information superiority.

Information is a strategic resource, vital to national security, and military operations depend on information and information systems for many simultaneous and integrated activities.

Information operations (IO) are described as the integrated employment of electronic warfare (EW), computer network operations (CNO), psychological operations (PSYOP), military deception (MILDEC), and operations security (OPSEC), in concert with specified supporting and related capabilities, to influence, disrupt, corrupt, or usurp adversarial human and automated decision making while protecting our own.

The purpose of this doctrine is to provide joint force commanders (JFCs) and their staffs guidance to help prepare, plan, execute, and assess IO in support of joint operations. The principal goal is to achieve and maintain information superiority for the US and its allies.

The information environment is the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information. The information environment is made up of three interrelated dimensions: physical, informational, and cognitive.

Core, Supporting, and Related Information Operations Capabilities

Core capabilities.

IO consists of five core capabilities which are: PSYOP, MILDEC, OPSEC, EW, and CNO. Of the five, PSYOP, OPSEC, and MILDEC have played a major part in military operations for many centuries. In this modern age, they have been joined first by EW and most recently by CNO. Together these five capabilities, used in conjunction with supporting and related capabilities, provide the JFC with the principal means of influencing an adversary and other target audiences (TAs) by enabling the joint forces freedom of operation in the information environment.

Supporting capabilities.

Capabilities supporting IO include information assurance (IA), physical security, physical attack, counterintelligence, and combat camera. These are either directly or indirectly involved in the information environment and contribute to effective IO. They should be integrated and coordinated with the core capabilities, but can also serve other wider purposes.

Related capabilities.

There are three military functions, public affairs (PA), civil military operations (CMO), and defense support to public diplomacy, specified as **related capabilities for IO**. These capabilities make significant contributions to IO and must always be coordinated and integrated with the core and supporting Information Operations capabilities. However, their primary purpose and rules under which they operate must not be compromised by IO. This requires additional care and consideration in the planning and conduct of IO. For this reason, the PA and CMO staffs particularly must work in close coordination with the IO planning staff.

Intelligence and Communications System Support to Information Operations

Successful planning, preparation, execution, and assessment of information operations (IO) demand detailed and timely intelligence.

Before military activities in the information environment can be planned, the current "state" of the dynamic information environment must be collected, analyzed, and provided to commanders and their staffs. This requires intelligence on relevant portions of the physical, informational, and cognitive properties of the information environment, which necessitates collection and analysis of a wide variety of information and the production of a wide variety of intelligence products.

Nature of IO intelligence requirements.

In order to understand the adversary or other TA decision-making process and determine the appropriate capabilities necessary to achieve operational objectives, commanders and their staffs must have current data. This includes relevant physical, informational, and cognitive properties of the information environment as well as assessment of ongoing IO activities.

Intelligence considerations in planning IO.

Intelligence Resources are Limited. Commanders and their intelligence and operations directorates must work together to identify IO intelligence requirements and ensure that they are given high enough priority in the commander's requests to the intelligence community (IC).

Collection Activities are Legally Constrained. The IC must implement technical and procedural methods to ensure compliance with the law. Additionally, intelligence may be supplemented with information legally provided by law enforcement or other sources.

Intelligence Support to IO Often Requires Long Lead Times. The intelligence necessary to affect adversary or other TA decisions often requires that specific sources and methods be positioned and employed over time to collect the necessary information and conduct the required analyses.

Information Environment is Dynamic. Commanders and their staffs must understand both the timeliness of the intelligence they receive and the differing potentials for change in the dimensions of the information environment.

Properties of the Information Environment Affect Intelligence. Collection of physical and electronic information is objectively measurable by location and quantity. Commanders and their staffs must have an appreciation for the subjective nature of psychological profiles and human nature.

Responsibilities and Command Relationships

Joint Staff.

The Chairman's responsibilities for IO are both general (such as those to establish doctrine, provide advice, and make recommendations) and specific (such as those assigned in DOD IO policy). The Operations Directorate of the Joint Staff (J-3) serves as the Chairman's focal point for IO and coordinates with the other organizations within the Joint Staff that have direct or supporting IO responsibilities. The IO divisions of the Joint Staff J-3 provide IO specific advice and advocate Joint Staff and combatant commands' IO interests and concerns within DOD and interact with other organizations and individuals on behalf of the Chairman.

Combatant commands.

Commander, United States Strategic Command's (USSTRATCOM's) specific authority and responsibility to coordinate IO across area of responsibility (AOR) and functional boundaries does not diminish **the imperative for other combatant commanders to employ IO**. These efforts may be directed at achieving national or military objectives incorporated in theater security cooperation plans, shaping the operational environment for potential employment during periods of heightened tensions, or in support of specific military operations. It is entirely possible that in a given theater, the combatant commander will be supported for select IO while concurrently supporting USSTRATCOM IO activities across multiple theater boundaries.

Components.

Components are normally responsible for detailed planning and execution of IO. IO planned and conducted by functional components must be conducted within the parameters established by the JFC. At the same time, component commanders and their subordinates must be provided sufficient flexibility and authority to respond to local variations in the information environment. Component commanders determine how their staffs are organized for IO, and normally designate personnel to liaise between the JFC's headquarters and component headquarter staffs.

Subordinate joint force commanders.

Subordinate JFCs plan and execute IO as an integrated part of joint operations. Subordinate staffs normally share the same type of relationship with the parent joint force IO staff as the Service and functional components. **Subordinate JFC staffs may become involved in IO planning and execution to a significant degree**, to include making recommendations for employment of specific capabilities, particularly if most of the capability needed for a certain operation resides in that subordinate joint task force.

Organizing for joint IO.

Combatant commanders normally **assign responsibility for Information Operations** to the **J-3**. When authorized, the director of the J-3 has primary staff responsibility for planning, coordinating, integrating, and assessing joint force IO. **The J-3 normally designates an Information Operations cell chief** to assist in executing joint IO responsibilities. The primary function of the IO cell chief is to ensure that IO are integrated and synchronized in all planning processes of the combatant command staff and that IO aspects of such processes are coordinated with higher, adjacent, subordinate, and multinational staffs. To integrate and synchronize the core capabilities of IO with IO-supporting and related capabilities and appropriate staff functions, the IO cell chief normally leads an "IO cell" or similarly named group as an integrated part of the staff's operational planning group or equivalent. The organizational relationships between the joint IO cell and the organizations that support the IO cell are per JFC guidance.

Planning and Coordination

IO planning follows the same principles and processes established for joint operation planning.

The IO staff coordinates and synchronizes capabilities to accomplish JFC objectives. Uncoordinated IO can compromise, complicate, negate, or harm other JFC military operations, as well as other USG information activities. JFCs must ensure Information Operations planners are fully integrated into the planning and targeting process, assigning them to the joint targeting coordination board in order to ensure full integration with all other planning and execution efforts. Other USG and/or coalition/allied information activities, when uncoordinated, may complicate, defeat, or render DOD IO ineffective. Successful execution of an information strategy also requires early detailed JFC IO staff planning, coordination, and deconfliction with USG interagency efforts in the AOR to effectively synergize and integrate IO capabilities.

Planning considerations.

IO planning must begin at the **earliest stage** of a JFC's campaign or operations planning and must be an integral part of, not an addition to, the overall planning effort. IO are used in all phases of a campaign or operation. The use of IO during early phases can significantly influence the amount of effort required for the remaining phases.

The use of IO in peacetime to achieve JFC objectives and to preclude other conflicts, requires an ability to integrate Information Operations capabilities into a comprehensive and coherent strategy through the establishment of information objectives that in turn are integrated into and support the JFC's overall mission objectives. The combatant commander's theater security cooperation plan serves as an excellent platform to embed specific long-term information objectives

IO planning requires early and detailed preparation. Many Information Operations capabilities require long lead-time intelligence preparation of the battlespace (IPB). IO support for IPB development differs from traditional requirements in that it may require greater lead time and may have expanded collection, production, and dissemination requirements. Consequently, combatant commanders must ensure that IO objectives are appropriately prioritized in their priority intelligence requirements (PIRs) and requests for information (RFIs).

As part of the planning process, designation of release and execution authority is required. Release authority provides the approval for IO employment and normally specifies the allocation of specific offensive means and capabilities provided to the execution authority. Execution authority is described as the authority to employ IO capabilities at a designated time and/or place. Normally, the JFC is the one execution authority designated in the execute order for an operation.

IO may involve complex legal and policy issues requiring careful review and national-level coordination and approval.

Commander's intent and information operations.

The commander's vision of IO's role in an operation should begin before the specific planning is initiated. A commander that expects to rely on IO capabilities must ensure that IO related PIRs and RFIs are given high enough priority prior to a crisis, in order for the intelligence products to be ready in time to support operations. At a minimum, the commander's vision for IO should be included in the initial guidance. Ideally, commanders give guidance on Information Operations as part of their overall concept, but may elect to provide it separately.

Measures of performance and measures of

Measures of performance (MOPs) gauge accomplishment of Information Operations tasks and actions. **Measures of effectiveness (MOEs)** determine whether IO actions being executed are having the desired effect toward

effectiveness.

mission accomplishment: the attainment of end states and objectives. MOPs measure friendly IO effort and MOEs measure battlespace results. IO MOPs and MOEs are crafted and refined throughout the planning process.

Multinational Considerations in Information Operations

Every ally/coalition member can contribute to IO by providing regional expertise to assist in planning and conducting IO.

Allies and coalition partners recognize various IO concepts and some have thorough and sophisticated doctrine, procedures, and capabilities for planning and conducting IO. **The multinational force commander is responsible to resolve potential conflicts** between each nation's IO programs and the IO objectives and programs of the coalition. It is vital to integrate allies and coalition partners into IO planning as early as possible so that an integrated and achievable IO strategy can be developed early in the planning process.

Integration requirements include clarification of allied and coalition partner's IO objectives; understanding of other nations' information operations and how they intend to conduct IO; establishment of liaison/deconfliction procedures to ensure coherence; and early identification of multinational force vulnerabilities and possible countermeasures to adversary attempts to exploit them.

Information Operations in Joint Education, Training, Exercises, and Experiments

A solid foundation of education and training is essential to the development of IO core competencies.

The development of IO as a core military competency and critical component to joint operations requires specific expertise and capabilities at all levels of DOD. At the highest professional levels, senior leaders develop joint warfighting core competencies that are the capstone to American military power. The Services, United States Special Operations Command, and other agencies develop capabilities oriented on their core competencies embodied in law, policy, and lessons learned. At each level of command, a solid foundation of education and training is essential to the development of a core competency. Professional education and training, in turn, are dependent on the accumulation, documentation, and validation of experience gained in operations, exercises, and experimentation.

IO education considerations.

The IO career force should consist of both capability specialists (EW, PSYOP, CNO, MILDEC, and OPSEC) and IO planners. Both groups require an understanding of the information environment, the role of IO in military affairs, how IO differs from other information functions that contribute to information superiority, and specific knowledge of each of the core capabilities to ensure integration of IO into joint operations.

IO planners are required at both the component and the joint level.

Senior military and civilian DOD leaders require an executive level knowledge of the information environment and the role of IO in supporting DOD missions.

IO training considerations.

Joint military training is based on joint policies and doctrine to prepare joint forces and/or joint staffs to respond to strategic and operational requirements deemed necessary by combatant commanders to execute their assigned missions.

IO training must support the IO career force and be consistent with the joint assignment process. Joint IO training focuses on joint planning-specific skills, methodologies and tools, and assumes a solid foundation of Service-level IO training.

The Services determine applicable career training requirements for both their IO career personnel and general military populations, based on identified joint force mission requirements.

CONCLUSION

This document [JP 3-13] provides the doctrinal principles for DOD employment of IO. It has been designed to provide overarching guidance in the planning and execution of IO in today's joint/ multinational security environment. Its primary purpose is to ensure all of the capabilities comprising IO are effectively coordinated and integrated into our nation's warfighting capability against current and future threats.

Updated: October 2009

This Page Intentionally Blank

Joint Organizations and Educational Institutions

DEPARTMENT OF DEFENSE
UNITED STATES OF AMERICA
JOINT
STAFF
UNITED STATES
SPECIAL OPERATIONS COMMAND
UNITED STATES
STRATEGIC COMMAND
NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA
DEFENSE INFORMATION SYSTEMS AGENCY
UNITED STATES
JOINT FORCES
COMMAND
USJFCOM
JOINT INFORMATION OPERATIONS
WARFARE COMMAND
JOINT TASK FORCE
GLOBAL NETWORK OPERATIONS
JOINT SPECTRUM CENTER
DEPARTMENT OF DEFENSE
DEFENSE PROGRAM OFFICE
MISSION ASSURANCE
JOINT WARFARE ANALYSIS CENTER
JWAC
JOINT PSYCHOLOGICAL OPERATIONS SUPPORT ELEMENT
GLOBAL REACH ~ STRATEGIC IMPACT
JOINT FORCES STAFF COLLEGE
THAT ALL MAY LABOR AS ONE
NPS
PRAESTANTIA PER SCIENTIAM
1909

This Page Intentionally Blank

Joint Staff, Deputy Director for Global Operations (DDGO)

Mission:

The Deputy Director for Global Operations (DDGO) is responsible to the Director for Operations and the Chairman of the Joint Chiefs of Staff (CJCS) for providing expertise and advice in coordinating joint global operations to include information operations (IO). Within the DDGO, the Assistant Deputy Director for Information Operations (DDGO/IO) is responsible for IO activities, developing joint IO policy and doctrine, and coordinating with the Office of the Secretary of Defense (SecDef), combatant commands, Services, Defense Agencies, other staff directorates, the Intelligence Community, and interagency on IO issues/actions. In addition, the DDGO/IO is the focal point for all special technical operations (STO).

Organization:

The DDGO/IO contains five divisions:

The **Computer Network Operations Division (CNOD)** advises the CJCS, through the Director for Operations (DJ-3), on Cyberspace Operations. CNOD also supports Combatant Command (COCOM) plans and operational requests and interfaces with the U.S. government Interagency on operational employment and deconfliction of military CNO. Specific CNOD activities include:

- Planning and integration of CNO to support COCOMs through the Joint Operational Planning and Execution System (JOPES).
- Representing the Joint Staff at DoD and Interagency working groups, as necessary.
- Providing On-call support to the National Joint Operations and Intelligence Center and NMCC for Cyberspace issues.
- Providing input and oversight to exercises on the CJCS Exercise List and other major DoD and Interagency exercises with significant Cyberspace activities.

The **Information Operations Division (IOD)** facilitates and coordinates electronic warfare (EW) and special capabilities for the Chairman and in support of all COCOMs with the Office of the Secretary of Defense (OSD) and select interagency partners. Some of the tasks performed by IOD are:

- Support to COCOM requirements in EW and STO
- Train and Assist COCOM STO Cells to obtain JOPES approval
- Serve as the Joint Staff sponsor of Combat Camera assets
- Advocate IO related COCOM issues to the interagency
- Provide COCOMs with Science & Technology support for COA development

IOD consists of the following branches: Combatant Command Support, Plans Support, Electronic Warfare, Intelligence Community Liaisons, Science and Technology, and Strategic Multi-layer Analysis Management.

The **Program Support Division (PSD)** serves as the focal point for joint IO and STO policy and doctrine in support of CJCS priorities and COCOM requirements. As part of this mission, PSD is responsible for STO policies and programmatics, joint IO policy and doctrine coordination, and Joint IO Force oversight. Some of the tasks performed by PSD are:

- Develop and coordinate STO policies & procedures
- Develop and coordinate Joint IO policy & doctrine
- Coordinate Joint IO Force education and training requirements
- Provide global network & 24/7 Planning and Decision Aid System (PDAS) support

PSD consists of the following branches: Policy & Doctrine, Programs, Automated Information Systems/Budget, Network Support, and the PDAS Support Center.

The **Psychological Operations Division (POD)** develops and provides guidance to, and coordinates with, COCOMs and Services to plan and conduct Psychological Operations **(**PSYOP). Some of the tasks performed by POD are:

- Prepare, staff and transmit PSYOP specific execute orders, deployment orders, and PSYOP program approval
- Coordinate PSYOP activities with other US Government agencies
- Coordinate present and future manning & equipment issues

POD is composed of the Programs & Doctrine and the Combatant Command Support branches.

The **Special Actions Division (SAD)** develops and promulgates Joint policy and serves as the COCOMs' operational link to CJCS, SecDef and select interagency partners for Military Deception (MILDEC), Operations Security (OPSEC) and Defense Sensitive Support Activities. Some of the tasks performed by SAD are:

- Develop and coordinate MILDEC security policy
- Develop and coordinate OPSEC and MILDEC joint doctrine publications
- Serve as the Joint Staff focal point office for the Defense Sensitive Support Program
- Coordinate all Defense Sensitive Support requirements between OSD and other Government agencies with the Services and Combatant Commanders

SAD is composed of the Support Activities Branch and the Tactical Security Branch.

Location:

The DDGO is located within the Pentagon.

Website: http://www.dtic.mil/jcs/

Last Updated: September 2009

Joint Spectrum Center (JSC)

Challenge: Military spectrum is a finite resource. The high tempo of global military operations and subsequent logistical support strain the already overcrowded spectrum bands. Unmanned Arial Systems and satellite connections consume large amounts of available spectrum. The increased need for added capacity in voice, data, and image communications create a demand for deliberate and synchronized spectrum operations across the Department of Defense. The Joint Spectrum Center is at the forefront of spectrum operations and supports the warfighter by providing complete, one-stop spectrum-related services to the military departments and combatant commands.

Mission: To enable effective and efficient use of the electromagnetic spectrum and control of electromagnetic effects in support of national security and military objectives.

Major Responsibilities

- Provide operational support in spectrum matters to the Joint Staff and Combatant Commands for contingencies, operations, exercises, and otherwise as requested.

- Conducts research and development into spectrum efficient technologies to improve the Department's use of spectrum.

- Facilitates global spectrum information exchange by developing protocols, standards, applications, and information systems.

- Implements the DoD Joint Electromagnetic Environmental Effects (E3) Program.

- Develops, maintains, and distributes spectrum engineering and E3 analysis models, simulations, software, and data.

- Develops, distributes, and conducts E3 and spectrum management training courses for DoD Components.

- Provides technical E3 and spectrum engineering support, on a customer funded basis, to DoD, Federal Government organizations, the private sector when it is in the interest of national defense, and to foreign entities when authorized.

JSC Functional Components

J3 Operations Division. -- provides remote and/or deployed spectrum management training and support to the Joint Staff, Combatant Commands, and joint force commanders. Spectrum management support consists of spectrum-planning guidance, vulnerability analysis, environmental analysis, and interference resolution. Support is available for wartime and contingency operations, joint training exercises, and for operations other than war such as disaster relief operations.

J5 Research and Development Division. -- researches, assesses, and models emerging spectrum technologies, manages the DoD E3 program, provides E3 advice and training, develops electromagnetic spectrum models and databases, and provides spectrum policy technical advice and assessments.

J6 Spectrum Management Information Technology Division. -- supports the warfighter by providing and maintaining Spectrum Planning Services, E3 Models and Simulations, and Information Systems.

J8 Applied Engineering Division. -- provides technical (E3) and spectrum engineering analysis and test support on a customer-funded basis. This includes support to DoD and other Federal Government organizations; to the private sector when it is in the interest of national defense per 10 U.S.C. 2539b; and to foreign entities when authorized by the Foreign Military Sales Process through the Defense Security Cooperation Agency.

JSB Defense Spectrum Relocation Management Activity (DSRMA). -- provides technical analysis support to the Office of the Secretary of Defense, Networks and Information Integration, related to the relocation of DoD spectrum-dependent devices out of the 1710-1755 MHz frequency band. DSRMA initiatives include a portal and analysis capability to handle requests from commercial Advanced Wireless Service providers seeking early access to this frequency band, and two other projects: the Spectrum Management Technology Initiative (SMTI) and the Spectrum Technology Testbed Initiative (STTI). The SMTI is focused on improving the mathematical algorithms used by spectrum managers to nominate frequencies to fit new spectrum-dependent devices into increasingly congested spectrum environments, especially for systems being relocated. The STTI is a federation of spectrum management simulation tools used to test the viability of proposed relocation solutions in a realistic operational environment.

JSC Operational Support Services and Products

Warfighting Unified Combatant Commands and Joint Task Force (JTF) Commanders services include:

- Review of operations plans for spectrum supportability, upon request.
- Joint Spectrum Interference Resolution (JSIR) support through analysis and deployment teams as necessary.
- SPECTRUM XXI software training and joint exercise support.
- Liaison and coordination support to Information Operations (IO) and Joint Information Operations Center organizations.
- Engineering support to the Joint Staff in Navigational Warfare matters.

Communications-Electronics (C-E) Planning products and services are provided to the Assistant Secretary of Defense for Networks and Information Integration, Joint Staff, Unified Commands, JTFs, Military Departments, Defense Agencies, and directly to the warfighter, including:

- SPECTRUM XXI Frequency Nomination/Assignment/Allotment.
- Electronic Warfare (EW) deconfliction via Joint Restricted Frequency List (JRFL) creation and analysis.
- JRFL Assistance/Preparation.
- Interference Analysis.

- Propagation Predictions (MF-EHF).
- C-E System Performance Prediction.
- Radar Target Acquisition Coverage Prediction.
- Electromagnetic Compatibility Analyses in Support of Frequency Planning.
- Topographical Analyses.
- Joint Communications-Electronics Operating Instruction Planning/Preparation.
- Electromagnetic Environment Definition.
- Geophysical Environment Definition.

JSIR services are structured to have interference incidents resolved at the lowest possible level of the DoD component chain of command, using component organic resources to resolve interference incidents where possible. Those incidents that cannot be resolved locally are referred up the chain of command, with resolution attempted at each level.

If the interference incident cannot be resolved by the affected DoD Component or the service engineering agency responsible for spectrum interference resolution, then it is referred to the JSC JSIR office for resolution. The JSC JSIR office will analyze and attempt to recommend corrective action for reported interference problems by first using JSC databases and analytical tools, and then, if needed, by providing personnel and equipment to perform on-site direction finding, equipment test, and problem solution. If the assistance is requested for electronic attack incidents, the JSC JSIR office will coordinate analysis, collection, and field support activities with the appropriate agencies.

Command and Control (C2)-Protect services are provided through each of the following activities:

- Provision of databases on friendly force C2 system location and technical characteristics data for use in planning C2-protect. The databases cover DoD, US government, and civil communications, as well as radar, navigational aids, broadcast, EW, and identification systems. The databases are available on a quick reaction basis in a variety of formats and media to meet the needs of IO planners and spectrum managers.

- Assistance to the EW or IO officer in the development of the JRFL. The JSC provides an automated tool, SPECTRUM XXI, to assist in the development and management of the JRFL. The JSC has Unified Combatant Command support teams that deploy to the combatant command or JTF. The teams are available to prepare the JRFL or provide training and assistance in JRFL preparation. These teams are also available to provide assistance in spectrum management matters.

- Assistance in the resolution of operational interference and jamming incidents through the auspices of the JSIR Program.

- Provision of data on communications frequency and location data.

- Production of country studies. JSC Country Studies are published on CD-ROM and the internet, in support of Unified Combatant Command requirements. Each study provides information on civil telecommunications including: frequency management; broadcasting; telephone, telegraph, and telex; data communications; aeronautical communications; maritime communications; and transmission systems. Frequency allocations, assignments, histograms, and site location maps are also included. The frequency assignment data is provided in a spreadsheet compatible format and in vertical Standard Frequency Action Format (SFAF) compatible with SPECTRUM XXI.

Spectrum Regulatory Support services address the growth of commercial wireless services, such as Personal Communications Services, has greatly increased the demand for spectrum, and increased pressure for the government to relinquish portions of the spectrum to commercial interests. Continuing pressure to reallocate portions of the spectrum requires that the DoD have the ability to quickly assess the operational and economic impact of proposed reallocation legislation in order to defend critical DoD spectrum. The JSC draws upon a collection of databases and experience with spectrum management to respond to ad hoc inquiries. In addition, the JSC is positioned to develop in-depth assessments of various reallocation proposals that will provide all levels of government with the information needed to make responsible reallocation decisions.

Leadership: The command billet of the center (O-6) rotates between the Army, Air Force, and Navy. The JSC Commander reports to the Director, Defense Spectrum Organization who in turn reports to the DISA Vice Director.

Website: http://www.disa.mil/jsc/

Last updated: October 2009

Joint Warfare Analysis Center (JWAC)

Mission: provides combatant commands, Joint Staff, and other customers with precise technical solutions in order to carry out the national security and military strategies of the United States. JWAC maintains and enhances its ability to conduct comprehensive technical analysis. Over the past quarter of a century, JWAC has evolved from a small program office into a joint command of more than 600 personnel. As it grew, it became part of the Joint Chiefs of Staff in 1994 and then was spun-off as an independent joint command subordinate to Joint Forces Command (formerly Atlantic Command) in 1998.

Tasks:

- Provides Combatant Commander planners with full-spectrum analytical products in support of their objectives and guidance.
- Interfaces with the Joint Staff, national intelligence agencies, military commands, and governmental agencies to acquire necessary intelligence.
- Develops and adapts modeling and simulation technologies for analysis, computation, and the presentation of options to combatant commands, the Joint Staff, and other customers through partnership with various technology centers of excellence throughout DoD.
- Assesses strategic and operational planning processes including non-traditional methods for achieving national security objectives.

Capabilities:

- Maintains direct liaison staffs with Combatant Commanders, Joint Staff, DoD and non-DoD agencies. Liaison deploys in theater during crises and exercises.
- Researches political and socioeconomic conditions in countries of interest.
- Develops data-gathering and analysis methods and techniques to assess military, political, and socioeconomic impacts of U.S. military action and mathematical model and system simulations to support this analysis.
- Participates in development of new methodologies and technologies in support of joint experimentation, wargaming, and precision engagement.

Subordination: JWAC reports to the U.S. Joint Forces Command, Norfolk VA.

Leadership: Command of JWAC rotates between a Navy and Air Force O-6.

Personnel: The JWAC workforce is comprised of over 600 employees; approximately 500 are civilian and contractor positions, including multidisciplinary scientists, engineers, and analysts and the Command is authorized 62 military billets.

Location: JWAC is located at the Naval Support Facility, Dahlgren VA.

Note: The unclassified information above was obtained and approved by the JWAC for inclusion in this publication. Additional information may be obtained at:

Website: http://www.jwac.mil/

Last Updated: October 2009

U. S. Strategic Command (USSTRATCOM)

U.S. Strategic Command (USSTRATCOM) is one of ten unified commands in the Department of Defense. It is located at Offutt Air Force Base near Omaha, Neb. General Kevin P. Chilton commands USSTRATCOM, and serves as the senior commander of unified military forces from all four branches of the military assigned to the command. USSTRATCOM integrates and coordinates the necessary command and control capability to provide support with the most accurate and timely information for the President, the Secretary of Defense, other National Leadership and regional combatant commanders, and serves as steward and advocate of the nation's strategic capabilities.

USSTRATCOM promotes global security for America by deterring attacks on US vital interests and defending the nation should deterrence fail; leading, planning, and executing strategic deterrence operations; ensuring US freedom of action in space and cyberspace; delivering integrated kinetic and non-kinetic effects in support of US Joint Force Commanders; synchronizing global missile defense plans and operations, synchronizing regional combating of weapons of mass destruction plans; planning, integrating, and coordinating ISR in support of strategic and global operations, as directed; and advocating for capabilities as assigned.

The Command, including components, employs more than 2,700 people, representing all four services, including DoD Civilians and contractors, who oversee the command's operationally focused global strategic mission. The command is organized under a modified J-code structure as follows:

- **J0 The office of the Commander and the staff support agencies -** responsible for establishing the goals, mission, vision and leadership of the command. To help the commander, the immediate staff also includes the deputy commander in chief and a group of special advisors.

- **J1 (Manpower and Personnel) -** develops and administers USSTRATCOM command manpower and personnel policies, human resources, and personnel assignment programs.

- **J3 (Global Operations) -** coordinates the planning, employment and operation of DoD strategic assets and combines all current operations, global command and control and intelligence operations.

- **J2 (Intelligence) -** apprises the commander of foreign situations and intelligence issues relevant to current operational interests and potential national security policies, objectives and strategy. This includes providing indications, warning and crisis intelligence support, supporting unified command intelligence requirements, developing doctrine, developing joint architecture, coordinating support requirements and providing targeting support.

- **J3B (Current Operations) -** operates the Global Operations Center to provide the commander and the J3 with situational awareness, command and control, and integration across all mission areas. Conducts mission analysis, leads course of action development, and performs contingency and crisis action planning. Executes missions as directed by the Secretary of Defense and the President.

- **J4 (Logistics) -** Plans, coordinates and executes logistics functions for mobility, maintenance, engineering, readiness and sustainment and munitions management in support of command missions.

- **J6 (C4 Systems) -** coordinates, facilitates, monitors and assesses systems, networks and communications requirements.

- **J7 (Joint Exercises and Training) -** Manages USSTRATCOM Commander's Joint Training Program and Exercise Program in order to ensure readiness to perform the Command's Missions

- **J5 (Plans and Policy) -** responsible for coordinating the development and implementation of national security policy as it applies to the command and the execution of its mission. Develops future concepts and policy formulation for military space operations; global strike; information operations; global missile defense; and command and control, communications, computers, intelligence, surveillance and reconnaissance as outlined in the most recent Unified Command Plan. Integrates and synchronizes deliberate planning efforts across all USSTRATCOM missions. Prepares and maintains the nation's strategic nuclear war plan, and provides integrated global strike planning to deliver rapid, extended range, precision kinetic (nuclear and conventional) and non-kinetic (elements of space and information operations) effects in support of theater and national objectives. Performs day-to-day activities required for crisis-action and deliberate planning and execution, with updates to plans as necessary.

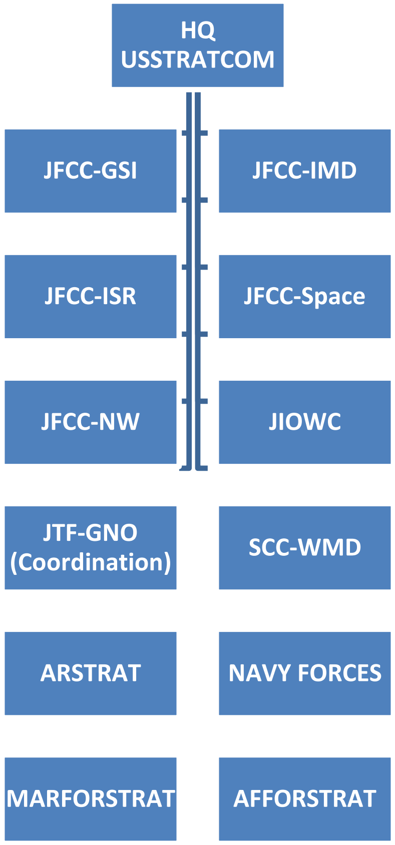
- **J8 (Capability and Resource Integration) -** conducts force management and analysis to include integrating, coordinating, prioritizing, and advocating USSTRATCOM future concepts, mission capability needs, weapons system development, support for emerging technologies, and command and control architecture across the mission areas. Responsible for the articulation and development of all command requirement processes to ensure that USSTRATCOM has the tools to accomplish its mission, and ensures appropriate decision support tools and assessment processes are in place to enhance operational capabilities. The directorate includes comptroller support, concepts and experimentation, and force assessments.

Global Innovation and Strategy Center (GISC) - The GISC mission is to produce knowledge discovery and shared understanding of strategic, operational and tactical perspectives to provide solutions to USSTRATCOM's toughest problems. The GISC is an academic facility that will bring together, in a cooperative effort, members of the public and private sector (military, political, academia, private sector, and media experts) and formalizes a process established soon after Sept. 11, 2001, with a focus on analyzing national and international security issues by leveraging expertise from the aforementioned elements of national power. This stimulates the development of innovative courses of action and comprehensive strategies to respond global threats against the United States.

USSTRATCOM exercises command authority over various task forces and service components in support of the command's mission. During day-to-day operations, service component commanders retain primary responsibility for maintaining the readiness of USSTRATCOM forces and performing their assigned functions. Their primary function is to provide organized, trained, and equipped forces for employment when called upon to support USSTRATCOM's global mission.

As the Department of Defense's key advocate for global capabilities, the command has extensive ties with defense agencies, the Department of Energy's national laboratories, and other sources of support. Through its many contacts and interagency relationships, the command facilitates planning, enhances information sharing between the military and other government agencies and streamlines decision making.

USSTRATCOM Functional Components, Service Components and Task Forces:



USSTRATCOM exercises command authority over five joint functional component commands (JFCCs) responsible for day-to-day planning and execution of primary mission areas: space and global strike; intelligence, surveillance and reconnaissance; network warfare; information operations; integrated missile defense; and combating weapons of mass destruction.

JFCC-Global Strike (JFCC-GS) -- optimizes planning, integration, execution and force management of assigned missions of deterring attacks against the U.S., its territories, possessions and bases, and should deterrence fail, by employing appropriate forces.

JFCC-Integrated Missile Defense (JFCC-IMD) -- develops desired characteristics and capabilities for global missile defense operations and support for missile defense. Plans, integrates and coordinates global missile defense operations and support (sea, land, air and space-based) for missile defense.

JFCC-Intelligence, Surveillance and Reconnaissance (ISR) (JFCC-ISR) -- plans, integrates and coordinates intelligence, surveillance and reconnaissance in support of strategic and global operations and strategic deterrence. Tasks and coordinates ISR capabilities in support of global strike, missile defense and associated planning.

JFCC-Space (SPACE) (JFCC-Space) -- optimizes planning, execution, and force management, as directed by the commander of USSTRATCOM, of the assigned missions of coordinating, planning, and conducting space operations.

JFCC-Network Warfare (NW) (JFCC-NW) -- facilitates cooperative engagement with other national entities in computer network defense and network warfare as part of global information operations.

Joint Information Operations Warfare Center (JIOWC) plans, coordinates, and, as directed, executes IO that cross areas of responsibility or that directly support national objectives, while supporting IO planning for other combatant commanders.

Joint Task Force-Global Network Operations (JTF-GNO) -- directs the operation and defense of the Global Information Grid to assure timely and secure net-centric capabilities across strategic, operational, and tactical boundaries in support of DoD's full spectrum of warfighting, intelligence, and business missions.

USSTRATCOM Center for Combating Weapons of Mass Destruction (SCC-WMD) -- plans, advocates and advises the commander, USSTRATCOM on WMD-related matters. Provides recommendations to dissuade deter and prevent the acquisition, development or use of WMD.

For More information please visit www.stratcom.mil

Last Updated: October 2009

Joint Task Force – Global Network Operations (JTF - GNO)

MISSION: A component of U.S. Strategic Command (USSTRATCOM), the Joint Task Force – Global Network Operations (JTF-GNO), is located in Arlington, VA. Under the authority of USSTRATCOM, JTF-GNO has the mission of directing the operation and defense of the DoD's Global Information Grid (GIG) to assure timely and secure Net-Centric capabilities across strategic, operational, and tactical boundaries in support of DoD's full spectrum of warfighting, intelligence, and business missions.

HISTORY: By the mid to late 1990's, it became increasingly apparent that the Global Information Grid, also known as the GIG, and the DoD computer networks that control and operate within it were becoming increasingly vulnerable to attacks. The so-called "information superhighway" was rapidly becoming a "cyber battlefield" where the protection previously afforded by traditional geographical boundaries was diminished, and a threat to a single DoD computer system was now potentially a threat to all DoD computer systems.

The DoD recognized this growing cyber threat and in response created the Joint Task Force for Computer Network Defense (JTF-CND). JTF-CND achieved initial operational capability (IOC) on 30 December1998 and full operational capability (FOC) in June 1999.

In October 1999, United States Space Command (USSPACECOM) assumed the CND Mission and JTF-CND was subordinated to it. In the fall of 2000, with the new Unified Command Plan (UCP) and the addition of an emerging Computer Network Attack (CNA) mission, JTF-CND began transforming into the Joint Task Force for Computer Network Operations (JTF-CNO).

JTF-CNO achieved IOC on 2 April 2001 and progressed towards achieving FOC on 1 October 2003. In October 2002, JTF-CNO was re-aligned under the United States Strategic Command (USSTRATCOM) under the new UCP, Change 2. JTF-CNO established itself as the premier DoD organization for intelligence analysis, planning, and operations of computer network warfare.

During its short history, JTF-CNO evolved from a handful of people to over 130 active duty military, civil service, and contracted employees. The JTF-CNO was instrumental in operationalizing computer network operations and defense for all of DoD. It also championed the CNA mission, working tirelessly to make this immature warfare area a viable part of our nation's ability to wage war.

In August 2003, JTF-CNO transformed its mission again with the transfer of the CNA mission to USSTRATCOM's Network Attack Support Staff (NASS). In January 2005, the mission to plan, integrate, coordinate and conduct CNA/CND, and integrate with CNE was given to Joint Functional Component Command – Network Warfare.

In June 2004, the JTF-CNO began its largest and most comprehensive transformation. On 18 June, the Secretary of Defense signed a delegation of authority letter designating the Director, Defense Information

Systems Agency (DISA) as the new Commander of Joint Task Force-Global Network Operations (JTF-GNO). With this designation, the new command assumed responsibility for directing the operation and defense of the GIG.

In July 2005, the JTF-GNO formed the Global NetOps Center (GNC) through the functional merger of elements from the JTF-CNO's Operations Directorate, DISA's Global Network Operations and Security Center (GNOSC), the DoD Computer Emergency Response Team (DoD-CERT), and the Global SATCOM Support Center (GSSC).

In May 2006, the UCP formally assigned CDRUSSTRATCOM the mission of directing GIG operations and defense-a mission subsequently assigned to the CDR JTF-GNO.

In November 2008, the Secretary of Defense directed CDRUSTRATCOM to place JTF-GNO under the operation control (OPCON) of the CDR JFCC-NW. This action was directed out of an urgent need to ensure a single command structure was empowered to plan, execute and integrated the full range of military cyberspace missions.

CURRENT OPERATIONS: The JTF-GNO performs its mission of directing the operations and defense of the GIG by using the NetOps construct that is outlined in its Joint Concept for GIG NetOps, Version 3, 4 Aug 06. NetOps is defined as the operational framework by which the CDRUSSTRATCOM, using his JTF-GNO component, will accomplish his assigned UCP (2006) mission of directing the operations and defense of the GIG. That framework consists of essential tasks, Situational Awareness, and Command and Control (C2). The essential tasks are GIG Enterprise Management (GEM), GIG Network Defense (GND), and GIG Content Management (GCM). Adhering to the responsibilities of the essential tasks (GEM, GND, and GCM) produces NetOps' desired effects of: Assured System and Network Availability, Assured Information Protection, and Assured Information Delivery in support of the overall goal of NetOps which is to provide the right information to the edge. NetOps and its essential tasks (GEM, GND, and GCM) include Information Assurance (IA) as defined and outlined in DODD 8500.1, Information Assurance, and CJCSI 6510.01E, Information Assurance and Computer Network Defense.

To execute these fundamental NetOps responsibilities, the CDR, JTF-GNO coordinates with Combatant Commands/Services/Agencies (CC/S/As). JTF-GNO has Operational Control (OPCON) over Service NetOps Components as provided in Forces For Memo, Feb 06, page IV-33, footnote 9 and stated in the Joint Concept of Operations for GIG NetOps, Version 3, 4 Aug 06. CDR, JTF-GNO also exercises Tactical Control (TACON) over the Service Computer Emergency / Incident Response Teams (CERTs/CIRTs) as provided in the Forces For Memo, Feb 06, page IV-33, footnote 9 and stated in the Joint Concept of Operation for GIG NetOps, Version 3, 4 Aug 06. To effectively operate the GIG as a global enterprise while realizing the Geographic Combatant Command (GCC) requirements to direct GIG operations in their theaters, CDRUSSTRATCOM developed an event-based C2 structure. C2 of GIG operations is based on the situation at the time. The three possible circumstances that determine the C2 of NetOps are known as global, theater, and non-global NetOps events. The preponderance of NetOps events are theater and are under the control of the GCC and their Service Components. Global and non-global NetOps events occur less frequently, but when they do occur, USSTRATCOM, using its JTF-GNO component, will direct the global response and respective CC/S/As will direct their non-global responses.

The Global NetOps Center (GNC) is the JTF-GNO Command Center responsible for executing the daily operation and defense of the GIG. The GNC provides the overall management, control, and technical direction for GIG NetOps and oversees a collaborative coordination process involving all Combatant Commands, Services, and Agencies, supporting the needs of the President, SECDEF, NetOps Community, and the warfighting, business, and intelligence domains.

Within each theater of operation, the JTF-GNO operates through Theater NetOps Centers (TNCs). The TNC is OPCON to JTF-GNO and offers onsite, theater support. Each TNC can issue technical directives to Service Theater Network Operations and Security Centers (STNOSCs)/Agency Theater Network Operations and Security Centers (ATNOSCs). The TNC develops, monitors and maintains a GIG SA view for the theater. The theater GIG SA view is aggregated and segmented based on requirements provided by the Theater NetOps Control Center (TNCC) as derived from the GIG common SA standards. The GIG SA view will include pertinent theater, operational, and tactical-level system and network views, GND, and GCM status.

The Service NetOps Component Commanders are the Commander, Space and Missile Defense Command/Army Strategic Command (1st IO Command/A2TOC); the Commander, 8th Air Force (AFNetOps Command); Commander, Fleet Forces Command (Navy Network Warfare Command (NAVNETWARCOM)); and Commander, US Marine Corps Network Operations and Security Command (MCNOSC). These Service Component Commanders exercise~~s~~ C2 over their respective Service Global Network Operations and Security Centers (SGNOSC).

The SGNOSCs and CERTs/ CIRTs serve as a part of the Service Component support to JTF-GNO. The SGNOSC and CERT/CIRT mission is to provide the Service-specific NetOps reporting and SA for the Service’s portions of the GIG. The SGNOSC and CERT/CIRT provide worldwide operational and technical support to the Service’s portions of the GIG across the strategic, operational, and tactical levels leveraging collaboration of the STNOSCs if established. The SGNOSC, in concert with the CERT/CIRT, are responsible for executing GND within their portion of the GIG, ensuring the Service's portions of GIG are secure and executing Service Title 10 enterprise responsibilities.

The Defense Agencies provide, operate, and maintain a large portion of the equipment, personnel, and other resources that make up the GIG. Execution of these functions requires the Agencies to be actively engaged in NetOps. To execute these functions, most Agencies have established NOSCs, which maintain SA of their portions of the GIG. The DoD Agencies that are not part of the Intelligence Community operate enterprise-wide systems as part of the GIG. These systems provide critical support to the DoD, COCOMs, and Military Services via their Agency Global NOSCs (AGNOSC). These AGNOSCs serve as a central point of contact for matters concerning the resources they provide to the GIG. DoD Agencies will align their AGNOSCs to provide USSTRATCOM visibility and insight of their GIG status and will follow the orders and directives issued by JTF-GNO per the 18 June 04 SECDEF Memo (modified by 17 Nov 05 DEPSECDEF Memo).

PERSONNEL: The JTF-GNO is currently authorized more than 350 positions.

Website: https://www.jtfgno.mil (PKI enabled website)

Website: www.stratcom.mil/fact_sheets/ (information only)

Last Updated: October 2009

This Page Intentionally Blank

Joint Information Operations Warfare Center (JIOWC)

Mission: The Joint Information Operations Warfare Center mission is to enable Information Operations (IO) and other missions for CDRUSSTRATCOM and other Joint Force Commanders as directed. JIOWC coordinates and synchronizes regional and global IO efforts and enhances IO support across the Department of Defense. Additionally, the JIOWC partners with other IO related entities, internal and external to the Department of Defense, to further enhance the global IO mission.

Tasks:

- Provide direct support to HQ USSTRATCOM
- Support USSTRATCOM Planning, Programming, Budgeting, and Execution efforts to include advocacy for EW, MILDEC, OPSEC, and Strategic Communication
- Conduct effects-based IO planning support and assessment
- Conduct and provide OPSEC survey and planning support (to include Joint Multi-Disciplinary Vulnerability Assessments) to USSTRATCOM and other Joint Force Commanders as directed
  Provide MILDEC planning support
- Provide Electronic Warfare planning support and advocacy
- Conduct effects-based assessment of assigned operations
- Maintain readiness at directed levels
- Participate in Joint Special Technical Operations (STO)
- Coordinate and integrate information operations intelligence preparation of the environment
- Assist in the development of joint IO doctrine and tactics, techniques, and procedures (TTP)
- Evaluate IO effectiveness in military operations
- Perform vulnerability/effectiveness analyses of US Advanced Concept Technology Demonstrations

Capabilities:

- Provides IO Subject Matter Experts with special emphasis on Electronic Warfare, Military Deception, and Operations Security
- Maintains a cadre of intelligence professionals tightly focused on the IO problem set
- Maintains a habitual working relationship with the IO staffs of the combatant commanders and service elements
- Provides focused and tailored IO planning products

History and Subordination: The Joint Electronic Warfare Center (JEWC) was established by the Secretary of Defense in October 1980 and reported to the Joint Staff. In September 1994, the mission was expanded and the organization was renamed the Joint Command and Control Warfare Center (JC2WC). In 1998, as a result of the Defense Reform Initiative (DRI), the JC2WC was realigned from the Joint Staff to US Atlantic Command. The JC2WC mission was further expanded and resulted in redesignation as the

Joint Information Operations Center (JIOC). In October 1999, the JIOC was realigned as a subordinate command of USSPACECOM. On 1 October 2002, the JIOC was realigned as a subordinate command to USSTRATCOM. In 2006 the JIOC was renamed the Joint Information Operations Warfare Command (JIOWC), and focused on operational IO planning and operations. Subsequently, the JIOWC was renamed the Joint Information Operations Warfare Center. The Director, JIOWC, reports to the Commander, USSTRATCOM.

Leadership: The Director of the JIOWC is a Defense Intelligence Senior Executive Service position that is filled by a competitive civil service selection process. Mr. Mark H. Johnson (DISES) is the Director of JIOWC, and USAR Colonel Vincent D. Crabb is the Deputy Director. The Strategic Advisor to the Director is Mr. Michael Furlong, Defense Intelligence Senior Leader (DISL).

Location: The JIOWC is co-located with the Air Force Intelligence, Surveillance & Reconnaissance Agency and components of 24th Air Force at Lackland AFB, TX in San Antonio, TX.

Website: http://www.jiowc.smil.mil

Last updated: October 2009

U. S. Special Operations Command (USSOCOM)

USSOCOM is one of the ten U.S. unified commands under DOD. It organizes, trains, equips and provides special operations forces to Geographic Combatant Commanders, American Ambassadors and their country teams. USSOCOM commands and controls all CONUS-based SOF from all four services. It also develops SOF-specific tactics, techniques, procedures, and doctrine, and conducts research, development, and acquisition of SOF-peculiar equipment. USSOCOM ensures its forces are trained and ready to respond to the call from the President, Secretary of Defense and the other nine combatant commanders as necessary.

Mission. USSOCOM provides fully capable Special Operations Forces to defend the United States and its interests. Synchronizes planning of global operations against terrorist networks.

Special operations are operations conducted in hostile, denied, or politically sensitive environments to achieve military, diplomatic, informational, and/or economic objectives employing military capabilities for which there is no broad conventional force requirement. These operations often require clandestine or discreet capabilities. Special operations are applicable across the range of military operations. They can be conducted independently or in conjunction with operations of conventional forces or other government agencies and may include operations by, with, or through indigenous or surrogate forces.

Special Operations Forces Core Tasks

Counter-proliferation of weapons of mass destruction (WMD) – actions taken to locate, identify, seize, destroy or capture, recover, and render such weapons safe.

Counterterrorism – measures taken to prevent, deter, and respond to terrorism.

Foreign Internal Defense – providing training and other assistance to foreign governments and their militaries to enable the foreign government to provide for its country's national security.

Special Reconnaissance – acquiring information concerning the capabilities, intentions and activities of an enemy.

Direct Action – short-duration strikes and other small scale offensive actions taken to seize, destroy, capture, recover or inflict damage in denied areas.

Psychological Operations – operations that provide truthful information to foreign audiences that influence behavior in support of U.S. military operations.

Civil Affairs Operations – activities that establish, maintain or influence relations between U.S. forces and foreign civil authorities and civilian populations to facilitate U.S. military operations.

Unconventional Warfare – operations conducted by, through, and with surrogate forces that are organized, trained, equipped, supported, and directed by external forces.

Information Operations – operations designed to achieve information superiority by adversely affecting enemy information and systems while protecting U.S. information and systems.

Counterinsurgency Operations – those military, paramilitary, political, economic, psychological and civic actions taken by a government to defeat insurgency.

Activities specified by the President or Secretary of Defense.

IO Core and Related Capabilities within USSOCOM Purview:

Psychological Operations (PSYOP)**.** A vital part of the broad range of U.S. political, military, economic, and information activities used by the U.S. government to secure national objectives, PSYOP disseminates truthful information to foreign audiences in support of U.S. policy and national objectives. Used during peacetime, contingency operations, and declared war, these activities are not a form of force, but are force multipliers that use nonviolent means in often violent environments. Persuading rather than compelling physically, they rely on logic, fear, desire or other mental factors to promote specific emotions, attitudes or behaviors. The ultimate objective of U.S. military psychological operations is to convince target audiences to take action favorable to the United States and its allies. The importance and effectiveness of psychological operations has been underscored during OPERATIONS ENDURING FREEDOM and IRAQI FREEDOM.

Civil Affairs (CA). CA units support military commanders by working to minimize the effect of civilians in the battle space and by coordinating with civil authorities and civilian populations in the commander's area of operations to lessen the impact of military operations on them during peace, contingency operations, and declared war. Civil Affairs forces support activities of both conventional and SOF, and are capable of assisting and supporting the civil administration in their area of operations. Long after the guns have fallen silent, the men and women of Civil Affairs continue to provide assistance to foreign governments, and to stabilize regions in turmoil.

Components. USSOCOM has four component commands and one sub-unified command:

1. U.S. Army Special Operations Command (USASOC). Located at Ft. Bragg, North Carolina. USASOC's mission is to organize, train, man, equip, educate, maintain combat readiness, and deploy assigned active duty and National Guard units of the Army Special Operations Force. Their mission is to accomplish special operations, psychological operations, and civil affairs operations. Their forces include:

- - 4th PSYOP Group (Airborne) (4th POG)
  - 95th Civil Affairs Brigade (Airborne)
- United States Special Forces Command (Airborne).
- John F. Kennedy Special Warfare Center and School.

75th Ranger Regiment

160th Special Operations Regiment (Airborne)

528th Sustainment Brigade (Airborne)

NOTE: Effective 1 Oct 06 the following units were reassigned from U.S. Special Operations Command (USSOCOM) to U.S. Joint Forces Command (USJFCOM):

- 350th, 351st, 352, and 353 Civil Affairs Commands (U.S. Army Reserve)
- 2nd POG and 7th POG (U.S. Army Reserve)

2. Naval Special Warfare Command (NAVSPECWARCOM). Located at Naval Amphibious Base, Coronado, CA. The mission of NAVSPECWARCOM is to organize, train, man, equip, educate, maintain combat readiness, and deploy assigned forces in support of joint and fleet operations worldwide. SEAL Teams are maritime, multipurpose combat forces organized, trained and equipped to conduct a variety of special operations missions in all operational environments and threat conditions. SEAL mission areas include direct action, counter-terrorism, special reconnaissance, foreign internal defense, information warfare, security assistance, counter-drug operations, personnel recovery, and hydrographic reconnaissance.

3. Air Force Special Operations Command (AFSOC). Located at Hurlburt Field, Florida. It provides Air Force Special Operations Forces to conduct and support global special operations missions. AFSOC's contribution to Information Operations is specifically in the form of the 193^{d} Special Operations Wing, Air National Guard. The wing operates the EC 130 "Commando Solo" which can broadcast television and radio programs directly to foreign audiences.

4. Marine Corps Forces Special Operations Command (MARSOC). Located at Camp Lejuene, NC. Activated February 2006, its primary mission is to organize, man, train and equip Marine Special Operations Forces. The MARSOC subordinate elements provide training to foreign militaries, conduct specified special operations missions like special reconnaissance, engage in direct action, provide intelligence support, coordinate supporting fires and provide logistical support to special operations task forces.

5. Joint Special Operations Command (JSOC). A sub-unified command of USSOCOM. JSOC provides a joint headquarters to study special operations requirements, ensures interoperability and equipment standardization, develops joint special operations plans and tactics, and conducts joint special operations exercises and training.

Location Address and Contact Information: Headquarters, United States Special Operations Command (HQ, USSOCOM)

- Headquarters, USSOCOM, 7701 Tampa Point Boulevard, MacDill Air Force Base, Florida 33621
- Public Affairs Office: (813) 826-4600

Website: http://www.socom.mil/

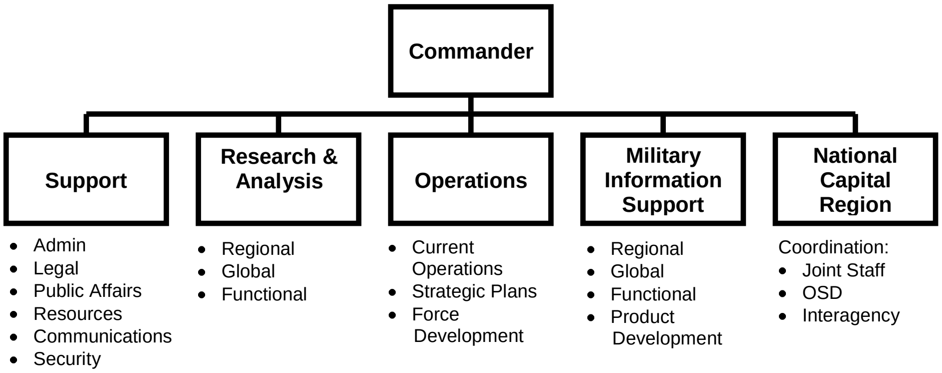
Last Updated: October 2009

This Page Intentionally Blank

Joint Military Information Support Command (JMISC)

History: The Joint Military Information Support Command (JMISC), formerly known at the JPSE or Joint PSYOP Support Element, is spearheading the Department of Defense's (DoD) information battle by developing programs and products designed to influence approved, large-scale foreign audiences in support of U.S. Government (USG) objectives in areas that cross Geographic Combatant Command (GCC) boundaries. The JPSE was established in 2003 and formally activated in 2006 at U.S. Special Operations Command (USSOCOM), Tampa, Florida. Shortly after September 11th, 2001, the Office of the Secretary of Defense (OSD) articulated a need for a strategic PSYOP capability within the DoD. The Defense Planning Guidance (FY 2004-2009) tasked Commander, USSOCOM to create a "Strategic PSYOP Force." The 2003 DOD Information Operations Roadmap directed the creation of "a Joint PSYOP Support element." The JPSE was renamed the JMISC on November 2007 to better characterize the strategic mission to support the interagency, OSD and GCCs. The senior military and civilians assigned to the JMISC strive to serve as the premier strategic PSYOP force within the DOD, focused at the global and trans-regional level, which provides effective and timely support to promote U.S. goals and objectives. The JMISC does so by using traditional and creative approaches, married with existing and emerging technologies, to reach and influence intended target audiences.

Mission: The Joint Military Information Support Command (JMISC) plans, coordinates, integrates and, on order, executes trans-regional and strategic psychological operations to promote U.S. goals and objectives. The JMISC operates by, with and through the GCCs and works closely with the interagency and Country Teams to identify the right means to connect with segments of the foreign population that the USG is most interested in reaching. The JMISC consists of functional, cultural, and regional experts that bring a "combined arms" approach to tackling what has become a tough, entrenched information war.


Commander

Support
- Admin
- Legal
- Public Affairs
- Resources
- Communications
- Security

Research & Analysis
- Regional
- Global
- Functional

Operations
- Current Operations
- Strategic Plans
- Force Development

Military Information Support
- Regional
- Global
- Functional
- Product Development

National Capital Region

Coordination:
- Joint Staff
- OSD
- Interagency

Commander's Intent: Using multi-media, broadcast within the culture and language of the intended audience in order to:

- Support the GWOT mission of CDR, USSOCOM; the Geographic Combatant Commands (GCCs), OSD and the interagency

  - Counter or defeat global terrorist ideology and influence
  - Deny safe-haven to terrorists abroad
- Work with and through Geographic Combatant Commands and other USG Agencies and Partner Nations
- Plan, develop, coordinate and integrate (synchronize) PSYOP at the strategic and trans-regional level

Characteristics:

- One of two brigade-level PSYOP units assigned to USSOCOM
- Comprised largely of senior military and civilian PSYOP personnel
- Manages and executes trans-regional information programs
- Develops DoD trans-regional PSYOP plans and can assist in developing GCC/JTF Strategic Communication, Information Operations, and PSYOP plans
- Coordinates/collaborates information activities with OSD and interagency partners
- Provides strategic & regional analysis and expertise
- Provides commercial-quality PSYOP product and prototype development

Source: Director of Operations, 813-826-0430/6620

Last Updated: September 2009

Joint Public Affairs Support Element (JPASE)

Mission: The Joint Public Affairs Support Element (JPASE) trains and maintains a public affairs professional capability to rapidly deploy as a team to assist the combatant commanders. The operational teams help to properly disseminate information to the public. JPASE seeks to enhance overall joint public affairs capabilities through not only training but also doctrine development, and the establishment of joint standards and requirements to assure the joint force commander has an organization of equipped, trained and ready public affairs professionals. The goal is for these professionals to provide counsel, operational planning and tactical execution of communication strategies as a function of joint military operations in support of national objectives. JPASE is located in U.S. Joint Forces Command's (USJFCOM) Joint Warfighting Center (JWFC) in Suffolk, Va.

JPASE Mission Statement: The Joint Public Affairs Support Element assures Joint Force commanders Public Affairs forces through joint capability development and training to plan and execute communication strategies in the joint, interagency and multinational environments. When directed, JPASE deploys in support of Combatant Commanders worldwide.

JPASE is organized to provide direct support to specific combatant command requirements. It replaces the former, *ad hoc* method of assembling teams to provide support. This new organization facilitates concentration on the particular aspects of geography, culture and organization of a specific command, while gaining proficiency and understanding of the common operating tools and practices each command employs. On order, JPASE deploys to the regional Combatant Commands in support of emergent joint operations as a trained, equipped and ready joint public affairs force. Its first deployment was during Hurricane Katrina in 2005. Forty-six of JPASE's 48 military and civilian personnel, drawn from all services, are designated to support expeditionary operations.

Organization: JPASE is organized around three objective areas:

1. Proponency Division**:** The Proponency Division is responsible for developing and sustaining capability improvements across the areas of doctrine, organization, training, materiel, leadership & education, personnel, and facilities, and is divided into seven functional areas:

- Concept development and experimentation
- Visual information development
- Public affairs collaborative information environment/Web portal management
- Lessons learned
- Education development
- Doctrine and Policy
- Capabilities

2. Operations and Training Division**:** The operations and training division is responsible for training public affairs and operational staffs includes four teams, geographically aligned with the unified commands, providing public affairs training, media simulation, staff assistance and exercise support to those commands.

3. Expeditionary Capability**:** The JPASE provides a standing, rapidly-deployable, turn-key joint public affairs capability to support a variety of operational requirements. Each of the operational training teams form the core of a Scalable Public Affairs Response Capability (SPARC) – a ready, mission tailored force package, to support exercises and to deploy in support of the combatant commands for operations and contingencies. COCOMs must provide logistics and life-support to each SPARC. At full operational capability (FOC) JPASE can deploy up to 24 persons for 90 days or 16 for 179 days and still maintain its ability perform all its mission essential tasks.

Reserve Components Capability: USJFCOM established a reserve joint public affairs unit (JPASE-R), in October 2004 to support and augment the active duty JPASE organization. It is trained and equipped to provide training and support for the active JPASE force during day-to-day operations and when it is deployed in support of emergent and contingency operations. It will be certified to deploy in support of operations, in whole, in part, or as individual augmenters.

Website: JFCOM Joint Warfighting Training Center: http://www.jfcom.mil/about/abt_j7.htm

Last Updated: October 2009

Joint Forces Staff College Information Operations Program

The Joint Forces Staff College (JFSC) was established in 1946 to better equip personnel from all of the services to function in the modern joint and combined warfare environment. It pre-dates the creation of the unified Department of Defense, and is the successor of the Army and Navy Staff College, established in 1943 for the same purpose. The college is located at the U.S. Naval Base, Norfolk, Virginia.

IO Education at JFSC. Department of Defense Instruction (DODI) 3608.12, " Joint Information Operations (IO) Education", (4 Nov 05) specifies that, "Joint Forces Staff College [will] develop and conduct a Joint IO planners course to prepare students to integrate IO into plans and orders on joint warfighting staffs". The College also offers an orientation course. Both are conducted by the Information Operations Division of the Joint Command, Control & Information Operations School (JC2IOS), and are outlined below.

1. Joint IO Orientation Course (JIOOC)

A one week course with the objective to educate and train U.S. Government (USG) personnel in the military grades of Lieutenant/Captain (O-3) to Captain/Colonel (0-6) and civilian equivalents in the basics of joint Information Operations (IO). Primary emphasis is at the Combatant Command level. The course focuses on teaching joint IO doctrine and DoD IO policy guidance as they apply to the operational level of joint warfare. It is particularly relevant to those serving in support of IO cells and other staff positions that require a basic knowledge of Joint IO. If IO planning skills are desired, then the student should take the JIOPC.

It gives students a common baseline of IO knowledge upon which to build practical skills and abilities to employ IO tools and techniques. In this one-week course, students are exposed to four blocks of instruction: Strategy; Intelligence support; IO Capabilities (Core, Supporting and Related); and Organization, Training, and Equipping. Each block of instruction includes a combination of instructor lecture, guest speaker presentations, guided discussions and/or panel discussions.

2. Joint Information Operations Planning Course (JIOPC)

A four week course for the purpose of establishing a common level of understanding for IO planners and IO capability specialists, between the ranks of 0-4 through 0-6, and DoD Civilian equivalents, who will serve in joint operational-level IO billets. *This course is required for Joint IO Career Force personnel assigned to a combatant command or JTF staff* (See CJCSM 1630.01, Joint Information Operations Force, 16 Mar 09).

The objective of the JIOPC is to educate and train military students between the ranks of 0-4 through 0-6, and DoD Civilian equivalents, to plan, integrate, and synchronize full spectrum IO into joint operational-level plans and orders. The school accomplishes this through class presentations, guest lectures, case studies, and practical exercises in a joint seminar environment. Students will be assigned to a working group consisting of approximately eight to ten individuals led by a faculty mentor. The course focuses on the following learning areas:

- Joint Operational Planning Process (JOPP)
- Joint Intelligence Preparation of the Environment (JIPOE)
- Information Operations (IO) Planning
- Interagency Planning & Coordination

Throughout the course the students use traditional planning methodologies within the joint planning community. The course is based upon joint doctrine that is reinforced, when necessary, by a compilation of various tactics, techniques, and procedures from throughout the department of defense.

The JIOPC is only taught in residence at the Joint Forces Staff College.

The JC2IOS Division of JFSC also offer Mobile Training Teams (MTT's) to commands needing orientation training. MTT's are funded by the host.

For information regarding the JFSC Information Operations Division, contact JC2IOS-IO@jfsc.ndu.edu or at 757-443-6333/6339 (DSN: 646).

Web Site:

http://www.jfsc.ndu.edu/

Last Updated: November 2009

Information Operations Center of Excellence, Naval Postgraduate School

NPS is located in Monterey, CA and is the successor to the Postgraduate Department of the U.S. Naval Academy, established at Annapolis, MD prior to World War One. Congress established the school as a full degree-granting institution in 1945, and it moved to its present location in 1951. The present student body numbers approximately 1,800, with representatives from all service branches, and the services of more than 25 allied nations. It grants degrees at the masters and doctorate levels.

Information Operations Center for Excellence. Mission. The President, Naval Postgraduate School (NPS) was tasked by Department of Defense Instruction (DoDI) 3608.12, ("Joint Information Operations (IO) Education" - 4 Nov 05) with establishing a DoD "Center of Excellence" (CoE) for Information Operations.

The IO CoE functions under the sponsorship of Commander, US Strategic Command (USSTRATCOM) to inform and support the development of innovations in Information Operations related policy, doctrine, technology and education.

Information Operations Education at NPS

1. Information Systems and Operations (ISO) Academic Certificate Program. NPS offers this certificate program in an asynchronous online mode. It is a part of its Master of Science (MS) degree in Information Systems and Operations (ISO) offered through the Information Sciences Department, The certificate program consists of four-courses given via Distributed Learning (DL). These four courses are:

SS3011 - Space Technology and Applications

IO3100 - Information Operations

IS3502 - Computer Networks: Wide Area/Local Area (Intro to Information Systems Networks)

CC3000 - Intro to Command, Control, Communication, Computer and Intelligence Systems in DoD

ISO Academic Certificate Website: http://www.nps.edu/DL/Cert_Progs/ISO.asp

2. Master of Science in Information Systems and Operations (Curriculum 356). This curriculum, offered through the Information Sciences Department, is a war-fighter oriented, in-residence MS degree, program that will provide fundamental graduate education to integrate information technologies, command and control processes, and IO methods and elements into innovative operational concepts for Information Operations in the context of Network Centric Warfare.

The Information Systems & Operations graduate will be able to:

- Innovatively create IO strategies and policies.
- Establish agile organizational structures and decision processes responsive to real time mission and situation requirements.
- Understand information technology and systems as enabling the acquisition of information and knowledge superiority leading to effective development and performance of information operations.
- Integrate technology, organization, policy and strategy into an Information Operations framework useful in both deliberate and crisis planning across the range of military operations;
- Identify and solve significant information operations problems and communicate the results in written reports and command briefings.

Website: Information on Naval Postgraduate School's ISO program can be obtained at the following site: http://www.nps.edu/DL/NPSO/cert_progs/iso.html

3. **Master of Science in Information Warfare Systems Engineering (Curriculum 595).** Graduates of this curriculum are thoroughly knowledgeable in Information Operations (IO) and Information Warfare (IW). They receive a Master of Science in Information Warfare Systems Engineering (MSIWSE) degree that provides the services with officers who are well versed in the technical, theoretical, and operational aspects of interdisciplinary IO/IW as they relate to joint mission objectives in modern warfare. This curriculum is sponsored by Commander, Naval Network Warfare Command and N6.

Website: Information on Naval Postgraduate School's MSIWSE program can be obtained at the following site: http://www.nps.edu/Academics/GeneralCatalog/414.htm#o436

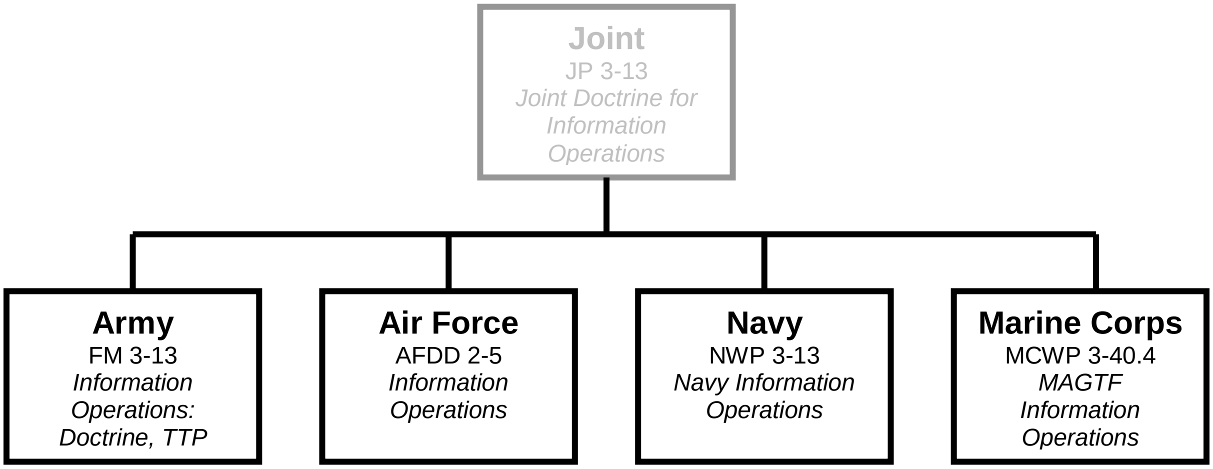
4. **Master of Science in Joint Information Operations (Curriculum 698.)** The Joint Information Operations curriculum educates military personnel and civilian officials in the strategic and operational dimensions of information relative to the use of force as an instrument of statecraft. Graduates will be able to develop information strategies to support military action by taking advantage of information technology, exploiting the growing worldwide dependence on automated information systems and capitalizing on near real time global dissemination of information to affect adversary decision cycles with the goal of achieving information superiority. This capability is possible only after students develop a thorough understanding of the enduring nature of war.

The curriculum is designed for both the specialist who will be assigned to an information operations position and the generalist who will be assigned to an operations directorate. The curriculum includes a core of military art and operations, the human dimension of warfare (psycho-social), analytical methods, and a technical sequence customized for each student. Additionally, each student will have an elective sequence designed to further develop an in-depth understanding of joint information operations. Graduates are awarded a Master of Science in Joint Information Operations. The program is 18 months long and requires a completed thesis.

Website: Information on the JIO Curriculum can be obtained at the following site: http://www.nps.navy.mil/da/.

Last Updated: October 2009

Service Information Operations Doctrine



Joint
JP 3-13
Joint Doctrine for Information Operations

Army
FM 3-13
Information Operations: Doctrine, TTP

Air Force
AFDD 2-5
Information Operations

Navy
NWP 3-13
Navy Information Operations

Marine Corps
MCWP 3-40.4
MAGTF Information Operations

This Page Intentionally Blank

Army Information Doctrine

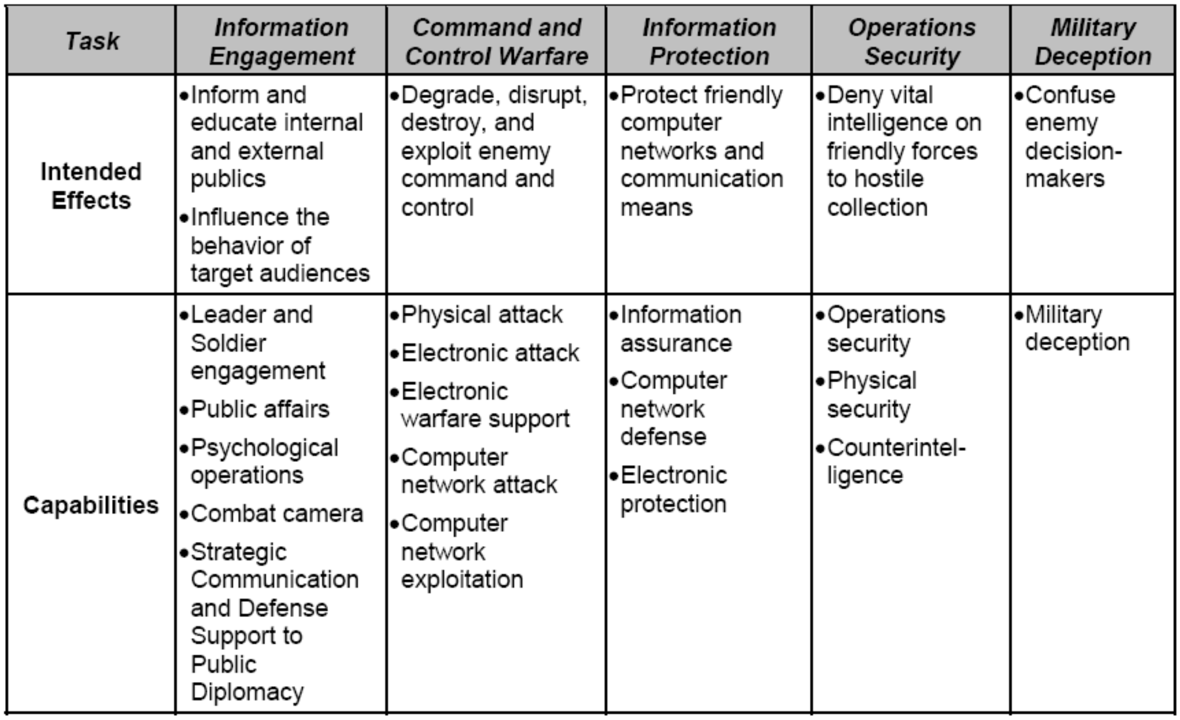
> *"At the time of the publication of the Information Operations Primer for AY10 the U.S. Army information doctrine update is currently on hold pending CSA guidance for road ahead. This section reflects the currently published doctrine in FM 3-0, FM 3-13 (NOV '03) and emerging IO doctrine."*

Key doctrinal documents: FM 3-0, *Operations* (28 February 2008) and FM 3-13*, Information* (TBP)

Full spectrum operations in today's operational environment require a comprehensive approach to information. In particular, Army operations emphasize the importance of peoples' perceptions, beliefs, and behavior to the success or failure of full spectrum operations and in the persistent conflicts the Nation continues to face. Enemies and adversaries will oppose friendly forces using every available information means, and they will exploit every advantage relentlessly. Army forces must protect friendly information and attack the opponents by using Army and joint capabilities. The Army conducts five information tasks to shape the operational environment. These are information engagement, command and control warfare, information protection, operations security, and military deception. (See Table 1.)

Today's operational environment yields a high and often decisive impact to the side which best leverages information. As a result, commanders provide personal leadership, direction, and attention to it, fully integrating information into battle command. They integrate information tasks into all operations and include them in the operations process from inception. They incorporate cultural awareness, relevant social and political factors, and other informational aspects related to their mission in their understanding and visualization of the end state and operational design. In their guidance and intent, commanders clarify the effects they intend to achieve by synchronizing information and other operational activities, to include identifying relevant audiences and the desired perceptual or behavioral effects on each. Commanders match information tasks with actions on the ground in their concept of operations. They ensure their staffs incorporate implementing actions into tasks to subordinate units, coordinating instructions, and other parts of plans and orders. Commanders acquire the best situational understanding through visiting units and talking with Soldiers and others involved in operations. They capitalize on this knowledge to adjust actions and information tasks to gain the desired effects. Finally, commanders understand the advantages of building partner capacity in this critical mission area; they promote informational activity and capability by, with, and through host-nation forces.

.



Task	*Information Engagement*	*Command and Control Warfare*	*Information Protection*	*Operations Security*	*Military Deception*
Intended Effects	•Inform and educate internal and external publics •Influence the behavior of target audiences	•Degrade, disrupt, destroy, and exploit enemy command and control	•Protect friendly computer networks and communication means	•Deny vital intelligence on friendly forces to hostile collection	•Confuse enemy decision-makers
Capabilities	•Leader and Soldier engagement •Public affairs •Psychological operations •Combat camera •Strategic Communication and Defense Support to Public Diplomacy	•Physical attack •Electronic attack •Electronic warfare support •Computer network attack •Computer network exploitation	•Information assurance •Computer network defense •Electronic protection	•Operations security •Physical security •Counterintel-ligence	•Military deception

Table 1.

The potential of information to generate powerful and perhaps unintended consequences can create a climate where risk aversion dominates decisionmaking related to information tasks. As a result, words and actions can fail to complement one another because there is no message, because the message is so neutral that it becomes irrelevant, or because the decision to employ a nonlethal capability is delayed until an opportunity is lost. Commanders overcome any such risk-averse tendencies by providing a clear, actionable, and achievable intent. They ensure that the timely and creative execution of information tasks is unhampered by overly cautious approval and control procedures.

Land operations occur among populations. This requires Army forces to contend constantly with the attitudes and perceptions of populations within and beyond their area of operations. Commanders use information engagement in their areas of operation to communicate information, build trust and confidence, promote support for Army operations, and influence perceptions and behavior.

INFORMATION ENGAGEMENT

***Information engagement* is the integrated employment of public affairs to inform U.S. and friendly audiences; psychological operations, combat camera, U.S. Government strategic communication and defense support to public diplomacy, and other means necessary to influence foreign audiences; and, leader and Soldier engagements to support both efforts.** Commanders focus their information engagement activities on achieving desired effects locally. However, because land operations always take place in a broader global and regional context, commanders ensure their information engagement plans support and complement those of their higher headquarters, U.S. Government strategic communication guidance when available, and broader U.S. Government policy where applicable.

Soldiers' actions are the most powerful component of information engagement. Visible actions coordinated with carefully chosen, truthful words influence audiences more than either does alone. Local and regional audiences as well as adversaries compare the friendly force's message with its actions. People measure what they see and what they experience against the commander's messages. Consistency contributes to the success of friendly operations. Conversely, if actions and messages are inconsistent, friendly forces lose credibility. Loss of credibility makes land forces vulnerable to enemy and adversary actions and places Army forces at a disadvantage. Synchronizing information engagement with the overall operation ensures the messages are consistent with the force's actions and actions amplify the credibility of those messages.

Leader and Soldier Engagement

Face-to-face interaction by leaders and Soldiers strongly influences the perceptions of the local populace. Carried out with discipline and professionalism, day-to-day interaction of Soldiers with the local populace among whom they operate has positive effects. Such interaction amplifies positive actions, counters enemy propaganda, and increases goodwill and support for the friendly mission. Likewise, meetings conducted by leaders with key communicators, civilian leaders, or others whose perceptions, decisions, and actions will affect mission accomplishment can be critical to mission success. These meetings provide the most convincing venue for conveying positive information, assuaging fears, and refuting rumors, lies, and misinformation. Conducted with detailed preparation and planning, both activities often prove crucial in garnering local support for Army operations, providing an opportunity for persuasion, and reducing friction and mistrust.

Public Affairs

Public affairs is a commander's responsibility to execute public information, command information, and community engagement directed toward both the external and internal publics with interest in the Department of Defense. Public affairs proactively informs and educates internal and external publics through public information, command information, and direct community engagement. Although all information engagement activities are completely truthful, public affairs is unique. It has a statutory responsibility to factually and accurately inform various publics without intent to propagandize or manipulate public opinion. Specifically, public affairs facilitates the commander's obligation to support informed U.S. citizenry, U.S. Government decisionmakers, and as operational requirements may dictate, non-U.S. audiences. Effective information engagement requires particular attention to clearly demarking this unique role of public affairs by protecting its credibility. This requires care and consideration when synchronizing public affairs with other information engagement activities. Public affairs and other information engagement tasks must be synchronized to ensure consistency, command credibility, and operations security.

The public affairs staff performs the following:—

- Advising and counseling the commander concerning public affairs.
- Public affairs planning.
- Media facilitation.
- Public affairs training.
- Community engagement.
- Communication strategies.

The public affairs staff requires augmentation to provide full support during protracted operations. (JP 3-61, AR 360-1, and FMs 46-1 and 3-61.1 govern public affairs.)

Psychological Operations

Psychological operations are planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals. The purpose of psychological operations is to induce or reinforce foreign attitudes and behavior favorable to the originator's objectives (JP 1-02). Commanders focus psychological operations efforts toward adversaries, their supporters, and their potential supporters. They may integrate these capabilities into the operations process through information engagement and the targeting process. Psychological operations units may also be task-organized with maneuver forces.

Combat Camera

Combat camera is the acquisition and utilization of still and motion imagery in support of combat, information, humanitarian, special force, intelligence, reconnaissance, engineering, legal, public affairs, and other operations involving the Military Services (JP 3-61). Combat camera generates still and video imagery in support of military operations. Combat camera units provide powerful documentary tools that support leader and Soldier engagement, psychological operations, and public affairs. For example, combat camera units can prepare products documenting Army tactical successes that counter enemy propaganda claiming the opposite.

Strategic Communication and Defense Support to Public Diplomacy

Strategic communication is focused United States Government efforts to understand and engage key audiences to create, strengthen, or preserve conditions favorable for the advancement of United States Government interests, policies, and objectives through the use of coordinated programs, plans, themes, messages, and products synchronized with the actions of all instruments of national power (JP 1-02). Strategic communication comprises an important part of the U.S. government's information arsenal. The government communicates themes and messages based on fundamental positions enumerated in the U.S. Constitution and further developed in U.S. policy. While U.S. leaders communicate some of this information directly through policy and directives, they also shape the environment by providing access and information to the media.

Defense support to public diplomacy is those activities and measures taken by the Department of Defense components to support and facilitate public diplomacy efforts of the United States Government (JP 3-13). Defense support to public diplomacy is a key military role in supporting the U.S. government's strategic communication program. It includes peacetime military engagement activities conducted as part of combatant commanders' theater security cooperation plans.

The Army implements strategic communication and defense support to public diplomacy while applying focused efforts to understand and engage key audiences. Such actions promote awareness, understanding, commitment, and action in support of the Army and its operations.

Responsibilities for Information Engagement

Commanders incorporate information engagement into full spectrum operations to impose their will on the operational environment. This requires commanders to be culturally astute; well-informed on the local political, social, and economic situations; and committed to leading the information engagement effort. Commanders direct multiple information engagement capabilities at those who affect or are affected by their operations. While doing so, they remain aware that, in an operational environment with pervasive connectivity and media presence, all messages ultimately reach all audiences. Spillover of a message intended for one audience to unintended audiences is inevitable. Dealing with the differing perspectives of diverse audiences requires thorough planning and continuously updated intelligence. Conducting full spectrum operations in the information age requires an accurate, complete, and clear understanding of each audience, including its interests, objectives, culture, and other nuances. Commanders reduce the natural ambiguity associated with this critical mission area by providing clear, actionable, and achievable intent and guidance.

Commanders integrate into information engagement into the operations process from inception, nesting information engagement activities with the intent of higher headquarters and with any applicable strategic communication guidance. They synchronize these activities with all other operational activity and integrate them into the operations process from inception. Finally, to prevent unintended consequences, commanders consider how actions proposed by the various staffs may affect the diverse audiences in the operational environment and their information engagement plan.

COMMAND AND CONTROL WARFARE

Information technology is becoming universally available. Most adversaries rely on communications and computer networks to make and implement decisions. Radios remain the backbone of tactical military command and control architectures. However, most communications relayed over radio networks are becoming digital as more computers link networks through transmitted frequencies. Additionally, adversaries are using civilian telecommunications, particularly cell phones and computer networks (including the Internet) to gather intelligence, disseminate information, shape perceptions and direct operations.

Command and control warfare i**s the integrated use of physical attack, electronic warfare, and computer network operations, supported by intelligence, to degrade, destroy, and exploit the adversary's command and control system or to deny information to it.** It includes operations intended to degrade, destroy, and exploit an adversary's ability to use the electromagnetic spectrum and computer and telecommunications networks. These networks affect the adversary's command and control or ability to communicate with an external audience. Command and control warfare combines lethal and nonlethal actions. These actions degrade or destroy enemy information and the enemy's ability to collect and use that information. The fires cell synchronizes physical attack, electronic warfare, and computer network operations against enemy and adversary command and control.

Physical attack disrupts, damages, or destroys adversary targets through destructive combat power. In support of command and control warfare, it uses lethal action to destroy or degrade enemy command and control. The most common form of attack is through fires, although the targeting cell may develop priorities that require ground maneuver or aviation attack. Synchronizing physical attack, electronic attack, and computer network attack through the targeting process and integrating them into operations is fundamental to successful command and control warfare.

Electronic warfare is any military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. Electronic warfare consists of three divisions: electronic attack, electronic protection, and electronic warfare support (JP 3-13.1). Of these, electronic attack and electronic exploitation directly support command and control warfare.

Electronic attack is that division of electronic warfare involving the use of electromagnetic energy, directed energy, or antiradiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability and is considered a form of fires (JP 3-13.1).

Electronic warfare support is that division of electronic warfare involving actions tasked by, or under direct control of, an operational commander to search for, intercept, identify, and locate or localize sources of intentional and unintentional radiated electromagnetic energy for the purpose of immediate threat recognition, targeting, planning and conduct of future operations (JP 3-13.1).

Computer network operations are operations comprised of computer network attack, computer network defense, and related computer network exploitation enabling operations (JP 3-13). Of these, computer network attack and computer network exploitation directly support command and control warfare.

Computer network attack consists of actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves (JP 3-13*). Computer network exploitation* are enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks (JP 3-13). Computer network defense is discussed under the information protection task. (See paragraph 7-33.)

Commanders use command and control warfare capabilities against an adversary's entire command and control system, not just the system's technical components. Although command and control warfare is primarily accomplished with physical and technical means, psychological operations and military deception activities can also provide important support, depending on the mission.

INFORMATION PROTECTION

Information protection **is active or passive measures that protect and defend friendly information and information systems to ensure timely, accurate, and relevant friendly information. It denies enemies, adversaries, and others the opportunity to exploit friendly information and information systems for their own purposes**. The secure and uninterrupted flow of data and information allows Army forces to multiply their combat power and sychronize landpower with other joint capabilities. Numerous threats to that capability exist in the operational environment. Information protection includes information assurance, computer network defense, and electronic protection. All three are interrelated.

Information assurance consists of measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities (JP 3-13).

Computer network defense consists of actions taken to protect, monitor, analyze, detect, and respond to unauthorized activity within the Department of Defense information systems and computer networks (JP 6-0). Effective network defense assures Army computer networks' functionality. It detects and defeats intruders attempting to exploit Army information and information systems. Commanders and staffs remain aware of and account for information on regulated (Department of Defense) and nonregulated (Internet) networks. They analyze how information from these mediums affects their operation; they take action to mitigate the associated risks.

Electronic protection is that division of electronic warfare involving actions taken to protect personnel, facilities, and equipment from any effects of friendly or enemy use of the electromagnetic spectrum that degrade, neutralize, or destroy friendly combat capability (JP 3-13.1).

OPERATIONS SECURITY

Operations security identifies essential elements of friendly information and evaluates the risk of compromise if an adversary or enemy obtains that information. This analysis compares the capabilities of hostile intelligence systems with the activities and communications of friendly forces and friendly information vulnerabilities. The analysis focuses on critical information that an adversary could interpret or piece together in time to be useful. Once identified, operations security experts prioritize friendly vulnerabilities and recommend countermeasures and other means of reducing the vulnerability. In some cases, the countermeasure cannot eliminate the risk, but it may reduce it to an acceptable level. Operations security includes physical security and counterintelligence. Physical security safeguards personnel, equipment, and information by preventing unauthorized access to equipment, installations, materiel, and documents while safeguarding them against espionage, sabotage, damage, and theft. Counterintelligence uses a wide range of information collection and activities to protect against espionage, combat other intelligence activities, protect against sabotage, and prevent assassinations. (JP 3-13.3 and FM 3-13 contain operations security doctrine.)

Operations security contributes to achieving surprise and completing the mission with little or no loss. Its absence contributes to excessive friendly casualties and possible mission failure. Information superiority hinges in no small part on effective operations security; therefore, measures to protect essential elements of friendly information cannot be an afterthought.

MILITARY DECEPTION

Military deception includes all actions conducted to mislead an enemy commander deliberately as to friendly military capabilities, intentions, and operations. At its most successful, military deception provokes an enemy commander to commit a serious mistake that friendly forces can exploit, there or elsewhere. However, effective military deception also introduces uncertainty into the enemy's estimate of the situation, and that doubt can lead to hesitation. Deception is a good means of dislocating an enemy force in time and space. Military deception can contribute significantly to information superiority; however, it requires integration into the overall operation beginning with receipt of mission. To achieve maximum effects, deceptions require good operations security, significant preparation, and resources for maximum effect. If added as an afterthought, deception often proves ineffective. Successful deception requires a reasonably accurate assessment of the enemy's expectations. (JP 3-13.4 and FM 3-13 contain military deception doctrine.)

INFORMATION IN CONTEXT

Commanders plan, prepare, execute, and assess the operational variables in order to leverage information as an element of combat power. Commanders integrate the Army Information Tasks throughout full spectrum operations to accomplish their mission. Combined with information management, knowledge management and intelligence, surveillance, and reconnaissance, the integration of Army Information tasks throughout the operation contributes to gaining and maintaining an operational advantage that leads to mission accomplishment and establishes a stable environment that sets the conditions for a lasting peace.

[The current version of FM 3-0, *Operations*, is available on line from the General Dennis J. Reimer Training and Doctrine Digital Library at:

atiam.train.army.mil/soldierPortal/atia/adlsc/view/public/7422-1/fm/3-13/toc.htm

The revised FM 3-13, Information (TBP), will be available once published.]

Last Updated: November 2009

This Page Intentionally Blank

Marine Corps Information Operations Doctrine

This U.S. Marine Corps IO doctrine overview reflects current U.S. Marine Corps MAGTF Information Operations doctrine (MCWP 3-40), under revision and scheduled to be published in Spring 2011, Joint IO (JP 3-13), and the key documents listed below.

Key documents:

- Marine Corps Order 3120.10, Marine Corps Information Operations Program (MCIOP), 30 June 2008.
- Marine Corps Information Operations Center: Concept of Operations for Information Operations Support to the Marine Air-Ground Task Force, 19 June 09.

Key doctrinal documents:

- MCWP 3-40.4, *MAGTF Information Operations*, 9 Jul 2003.
- MCWP 3-40.5, *Electronic Warfare*, 10 Sep 2002.
- MCWP 3-40.6 Psychological Operations (Dual Designated w/ Army)
- Other documents:
  - Marine Corps Order 3432.1, THE MARINE CORPS OPERATIONS SECURITY (OPSEC) PROGRAM
  - Marine Corps Bulletin 5400, CMC Washington DC CDI TFS 141153Z MAR 08, Establishment of MCIOC Phase One, 14 Mar 2008.

Fundamental changes in the global strategic environment have created conditions in which Information Operations (IO) will serve a critical role in achieving our military strategy and national security objectives. The Marine Corps IO Program seeks to integrate IO down to the lowest levels of the Marine Corps in order to deny or degrade the ability of hostile and non-hostile actors to disseminate their message and, if desired, to modify it to our benefit while simultaneously preventing those same hostile messages from negatively affecting our own decision-making processes. Integration of IO will be an essential part of routine operations in the expeditionary and joint environments.

Information Operations in Support of Expeditionary Warfare

Marine Corps information operations (IO) support maneuver warfare through the integration of all actions and information activities to deny, degrade, disrupt, destroy or influence an adversary commander's methods, means or ability to command and control (C2) his forces. IO enhances the ability of the MAGTF to project power during peace and war. They complement and facilitate the traditional use of military force but in some instances may stand alone, as a deterrent, for example. IO supports the integration of situational awareness, operational tempo, influence, and power projection to achieve advantage.

IO is a critical warfighting capability and integrating concept that facilitates the warfighting functions of C2, fires, maneuver, logistics, intelligence, and force protection. IO is not simply another "arrow" in the MAGTF commander's quiver. IO is a broad-based capability that "makes the bow stronger." Capabilities relevant to IO include, but are not limited to, the five core capabilities of IO--psychological operations (PSYOP), military deception (MILDEC), operations security (OPSEC), electronic warfare (EW), and computer network operations (CNO)—as well as the supporting and related capabilities such as Combat Camera (COMCAM), Public Affairs (PA), and Civil Affairs (CA). IO conducted by MAGTFs support battlespace shaping, force enhancement, and force protection activities.

MAGTFs will execute IO to enable and enhance their ability to conduct military operations consistent with the Marine Corps' capstone concept, *Expeditionary Maneuver Warfare (EMW)*. The MAGTF can support joint and multinational enabling by serving as an adaptive cornerstone force-bringing flexible command, control, communications, computers, and intelligence (C4I) systems that allow a follow-on joint or coalition force to be assembled in an expeditionary environment. The Marine Corps IO Center will increasingly provide MAGTF commanders with a continuous and scalable IO, PSYOP and reachback capability, allowing the MAGTF access to the resources of national level agencies and other service components.

Principles

- *IO is an integral function of the MAGTF.*
- *MAGTF IO is focused on the objective.*
- *The MAGTF commander's intent and concept of operations determine IO targets and objectives.*
- *MAGTF IO must be synchronized and integrated with those of the higher and adjacent commands*
- *MAGTF IO is supported by the total force.*
- *Many different capabilities and activities must be integrated to achieve a coherent IO strategy.*
- *Intelligence support is critical to the planning, execution, and assessment of IO.*

Staff Responsibilities

- The G-3/S-3 is responsible for IO. The future operations section, specifically MAGTF Fires and Effects is responsible for overseeing the planning and coordination of the IO effort. The MAGTF IO officer, within G-3/S-3 Effects Cell is responsible for:

  - The broad integration and synchronization of IO efforts.
  - Responding directly to the G-3/S-3 for MAGTF IO.
  - Ensuring that the IO cell provides input to the operational planning team (OPT) during planning to ensure coordinated operations.
  - Preparing the IO appendix to the operation order (OPORD).
  - Overseeing the core personnel within the IO cell as well as augmentees from external agencies.
  - Ensuring that all IO matters are coordinated within the MAGTF staff, higher headquarters, and external agencies.

- The electronic warfare officer (EWO) integrates EW operations through the EW coordination center (EWCC) or the IO cell when established.

Information Operations Cell

The IO cell is a task-organized group, established within a MAGTF and/or higher headquarters to integrate the core, supporting and related capabilities of IO. A fully functioning IO cell integrates these capabilities and considerations into all MAGTF operations through extensive planning and coordination among all the elements of the staff (i.e.: IO working group).

Information Operations Intelligence Integration (IOII). Intelligence provides the essential basis for planning IO through the following considerations:

- The adversary commander's freedom of action and the freedom of action allowed to subordinates including adversary perceptions of the situation and developments.
- Adversary IO capability, intent, morale, and vulnerability to offensive IO.
- C2 aspects such as key personnel, target audiences, headquarters, communications nodes, databases or intelligence collection systems. C2 nodes that appear in more than one adversary COA should be highlighted for targeting.
- Assessments of friendly vulnerability to adversary IO.
- Supporting the collection of information to assess the effectiveness of the IO program.

Information Operations Capabilities

Information Operations include all actions taken to affect decision maker information and information systems while defending friendly information and information systems. IO are focused on the adversary's key decision-makers and are conducted during all phases of an operation, across the range of military operations, and at every level of war. IO is an integrating function of all of these core, related and supporting capabilities, and is a component of strategic communications.

Note: The following *descriptions* are presented vice the *definitions* which in most cases are the respective Joint definitions found in JP 1-02.

- **Psychological Operations** (PSYOP) conveys selected information to shape attitudes and influence the behavior of foreign governments, organizations, groups, and individuals in the MAGTF's area of influence. The mere presence of Marine Corps forces may be a PSYOP activity in itself, influencing a situation through a display of purpose. Expeditionary PSYOP Teams (EPTs) from the Marine Corps IO Center will augment existing MAGTF PSYOP capabilities with PSYOP planning and limited distribution of products via radio, loudspeaker, face-to-face, etc.

- **Military Deception** (MILDEC) targets enemy decision makers by targeting their intelligence collection, analysis, and dissemination systems. Deception requires a thorough knowledge of adversaries and their decision making processes. Military deception is focused on achieving a desired behavior, not simply to mislead. The purpose is to cause adversaries to form inaccurate impressions about friendly force capabilities or intentions by feeding inaccurate information through their intelligence collection or information assets. The goal is to cause the adversary to fail to employ combat or support units to their best advantage. For MILDEC to be successful in the modern information environment, the information must be deconflicted with other information dissemination capabilities.

o **Electronic warfare** (EW) is coordinated by the EW Coordination Cell and more broadly by the IO Cell in order to maximize the effect of EW with other IO and MAGTF capabilities, and to prevent mutual interference. Successful military operations now greatly depend on control of the electromagnetic spectrum. The force that can deprive the enemy the use of the electromagnetic spectrum, exploit the enemy's use of the electromagnetic spectrum to obtain information for its own purposes, and control the electromagnetic spectrum will have an important advantage.

- **Operational Security** (OPSEC) is the key to information denial. It gives the commander the capability to identify friendly indicators that can be observed by adversary intelligence systems. These indicators could be interpreted or pieced together to derive critical information regarding friendly force dispositions, intent, and/or COAs that must be protected. The goal of OPSEC is to identify, select, and execute measures that eliminate or reduce, to an acceptable level, indications and other sources of information, which may be exploited by an adversary.

- **Computer Network Operations** (CNO) support C2 by facilitating the decision making process by providing communication and information systems that are reliable, secure, timely, and flexible. CNO protect information and information processes through computer network defense and IA activities. CNO may also be used to attack or exploit an adversary's information systems through computer network attack or exploitation. The Marine cryptologic support battalion or the RadBn may be tasked to support CNO activities. While the MAGTF does not have a CNA force, it must be aware of available joint capabilities.

IO Related Capabilities:

- **Physical Attack** applies friendly combat power against the enemy. It reduces enemy combat power by destroying enemy forces, equipment, installations, and networks. Within IO, the effects and messages sent by physical attacks are coordinated and synchronized in order to achieve the desired operational effects.

- **Information Assurance.** IA is information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. (JP-02). IA capabilities include information security.

- **Physical Security** contributes directly to information protection. Information, information-based processes, and information systems—such as C4 systems, weapon systems, and information infrastructures—are protected relative to the value of the information they contain and the risks associated the compromise or loss of information.

- **Counterintelligence (**CI) provides critical intelligence support to command force protection efforts by helping identify and counteract potential threats posed by hostile intelligence capabilities and by organizations or individuals engaged in espionage, sabotage, subversion or terrorism, while helping deceive the adversary as to friendly capabilities, vulnerabilities, and intentions. CI increases uncertainty for the enemy, thereby making significant contribution to MILDEC, PSYOP and the success of friendly operations. CI also identifies friendly vulnerabilities, and evaluates and assists in implementing appropriate security measures. Physical security reduces vulnerabilities. OPSEC reduces exposure.

- **Combat Camera** (COMCAM) is the acquisition and utilization of still and motion imagery in support of combat, information, humanitarian, intelligence, reconnaissance, PA and other operations. The still and video imagery and products gathered and produced by COMCAM are powerful tools that can support the countering of enemy propaganda, effectively informing and influencing target audiences, and gathering and analyzing intelligence.

IO Supporting Capabilities:

- **Public Affairs'** (PA) mission is to provide timely, accurate information to Marine-specific, American and global audiences, and to initiate and support activities contributing to good relations with the public. PA seeks to increase audiences' understanding of the Marine Corps' roles, missions and capabilities in order to gain and maintain domestic and international public support, elicit public approval, degrade enemy planning and actions, deter enemy aggression, and counter adversarial propaganda. While intents differ, PA and IO ultimately support the dissemination of information, themes and messages to various audiences, and thus must coordinate, synchronize and deconflict their operations.

- **Civil-Military Operations** (CMO) have become an integral element of military operations. Commanders must consider how their actions affect, and are affected by, the presence of noncombatants. Accordingly, through careful planning, coordination, and execution, CMO can help the MAGTF win by shaping the battlespace, enhancing freedom of action, isolating the enemy, meeting legal and moral obligations to civilians, and providing access to additional capabilities.

- **Defense Support to Public Diplomacy** (DSPD) consists of activities and measures taken by DoD components to support and facilitate public diplomacy efforts of the USG. IO integrates and synchronizes the actions and information activities of the MAGTF with those of the Department of State. IO, as part of DSPD, supports the synchronization of the elements of national power and military operations nested within higher's and the USG's strategic communication plan.

MAGTF Commanders and Marines naturally understand IO are important in today's operating environment and are frequently aware of the various messages they are sending, both in words and actions. It is the mission of IO, and the Marine Corps IO Center in particular, to enhance this understanding with informed knowledge; to support MAGTF commanders and Marines on the ground with the appropriate personnel, equipment and resources; and to integrate and synchronize Marine actions, information and communications to accomplish the MAGTF mission.

For more information contact Capt Shawn M. Mercer at 703-784-5115 or email at shawn.m.mercer@usmc.mil.

Updated: October 2009

This Page Intentionally Blank

Navy Information Operations Doctrine

Key doctrine and tactics, techniques, and procedures

- NWP 3-13, *Navy Information Operations*, June 2003 (in revision)
- NTTP 3-13.1, *Theater and Campaign Information Operations Planning*, April 2008
- NTTP 3-13.2, *Navy IO Warfare Commander's Manual*, May 2006 (in revision)
- Other key TTP:
  - NTTP 3-51.1, *Navy Electronic Warfare (Feb 06)*
  - NWP 3-53 *Navy Psychological Operations*
  - NTTP 3-54/MCWP 3-40-9 *Operations Security*, Mar 09
  - NTTP 3-58.1, *Multi-Service Military Deception Planners Guide* (April 2007)
  - NTTP 3-58.2, *Navy Military Deception*, April 2009
  - NTTP 3-51.2, *Multi-Service Reprogramming at Sea of Electronic Warfare and Target Sensing Systems*, January 2007 (in revision)
  - NWP 3-63, *Navy Computer Network Operations* Vol 1 (April 2008)
  - NWP 3-63 *Navy Computer Network Operations* Vol 2 (Sep 2008)
  - NTTP 3-13.6 Countering Counter Intelligence, Surveillance, Reconnaissance, Targeting (in development)
  - NTTP 3-51.3 Communications Electronic Attack (in development)
  - TM 3-01.1-07 Integrated HardKill and Softkill Tactics in Antiship Missile Defense
  - NTTP 3-13.5 Navy Cryptologic Operations (in development)

- **Fleet Concept of Operations (CONOPS)**
  - Fleet Information Operations, December 2006 (in revision)
  - Maritime Influence, August 2007
  - Maritime Headquarters-Maritime Operations Center (MHQ-MOC), March 2007

- **NWPs, NTTPs, TACMEMOs, and CONOPS are available at:** http://www.nwdc.navy.smil.mil under the Navy Doctrine Library System link

Summary of Navy Information Operations Doctrine and Concepts

- The planned revision to NWP 3-13 Navy Information Operations have been placed on hold awaiting JP 3-13 ongoing revisions.
- The effects of the establishment of JOINT CYBER COMMAND and the supporting FLEET CYBER COMMAND are not currently reflected in Navy IO TTP and CONOPS and are not addressed in this summary

- When NWP 3-13 is completed the new document can be found at http://www.nwdc.navy.smil.mil under the Navy Doctrine Library System link.

Introduction

The United States (U.S.) has experienced a shift from strictly symmetric, or force-on-force, warfare to more asymmetric warfare and military operations. Many of today's adversaries rely primarily on operations such as terrorism, disinformation, and propaganda campaigns to circumvent or undermine U.S. and allied strengths and exploit friendly vulnerabilities. Future Navy forces will continue to face adversaries outside the generally accepted force-on-force environment of the past. Naval forces are challenged by asymmetric operations in all domains—surface, subsurface, air, ground, and cyberspace—and must therefore defend against, defeat, deny, or negate the capabilities that will be used to prevent U.S. freedom of access. Information Operations (IO) is applicable across the range of military operations, (e.g., supporting major combat operations, global war on terrorism, etc.), in support of the Navy operating concept. Furthermore, the Navy must provide IO capabilities, organizational structures, planning processes, and personnel to maritime headquarters (MHQs)/joint force maritime component commanders (JFMCCs) engaged in theater security cooperation plans (TSCPs) and/or combat operations that enable our forces to engage in the asymmetric domain. Rapid advances in information technology provide today's military with unparalleled abilities to collect, process, and disseminate information. Technological advances have also increased the commander's vulnerability as a target for adversary information collection, shaping, and attack. IO will continue to play a key role by allowing the Navy and its partners to dominate warfare in the maritime domain. Operations within this domain include controlling the sea, conducting operational maneuvers throughout the world, deterring aggression through forward presence and influence operations in peacetime, responding to crisis, conducting major combat operations, and complementing other instruments of national power by projecting power from the sea, directly and decisively influencing events ashore.

Core Capabilities of Information Operations

IO was established as a warfare area within the Navy with the goal of affecting accuracy, usability, timeliness, completeness, or relevance of information used in guiding and conducting operations. IO includes electronic warfare (EW), computer network operations (CNO), psychological operations (PSYOP), military deception (MILDEC), and operations security (OPSEC). Supporting capabilities of IO include physical attack, physical security, information assurance, public affairs (PA), combat camera/visual information, civil-military operations, legal affairs, meteorology, intelligence, and oceanography. This is Navy IO at its most fundamental level and could consist of a wide (almost unbounded) array of "weapons," within the core, supporting, and related capabilities above.

IO is an integral part of the Navy planning and targeting process that continues through the range of military operations (see Figure 1). From guiding effects-based planning in the earliest stages to the weaponeering assessment phase of the targeting cycle, IO planners can assist in determining the right mix of maneuver, and kinetic/nonkinetic weapons that will produce the commander's desired effect. In addition to offering nonkinetic options to traditional strike warfare, IO plans often require the use of strike group maneuvers (concentration of forces and presence), kinetic strikes, and special operations warfare to deny, disrupt, destroy, or degrade information systems to attain overall campaign objectives. While each capability of IO includes a specialized planning process and can be applied to military operations individually, their coordinated application maximizes friendly advantages.

Information Operations Fundamentals

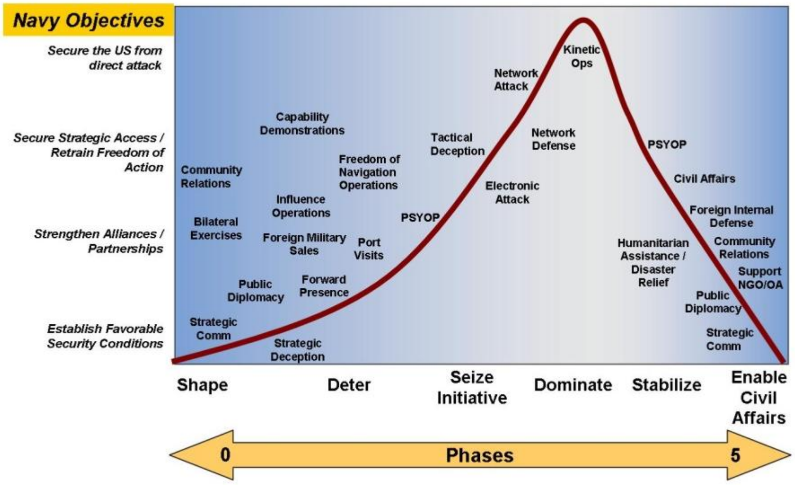


Figure 1. Range of Military Operations Integrating IO

Information Superiority

- Information superiority embodies the ability to collect, process, and disseminate the correct information to the right person, at the right place and time, in the right form, while denying an adversary the ability to do the same. Network-centric operations can foster information superiority by networking sensors, decisionmakers, and shooters. The goal of using network-centric operations is to increase mission effectiveness in order to achieve an increased state of readiness.

This superiority contributes to the ability to project maritime power forward from the sea, and ultimately in all warfighting domains. IO supports information superiority by corrupting, deceiving, delaying, denying, disrupting, degrading, or destroying one of the dimensions of information before it is presented to the adversary's commander, while protecting the same friendly information dimensions. Enabled through FORCENet (discussed later), information superiority is achieved through effects-based approach to operations, maritime power projection, maritime influence, target development, and environmental awareness and shaping (EAS). All echelons and warfare areas strive for and plan to achieve and maintain information superiority through coordinated efforts among the operations, intelligence, and command, control, communications, and computers (C4), and knowledge management.

Effect-Based Approach to Operations

An effects based approach to operations focuses on improving the commander's ability to affect an adversary's behavior and/or capabilities through the integrated application of select instruments of national power (diplomatic, information, military, economic). Effects are created to achieve objectives and are characterized as the physical and/or behavioral state of political, military, economic, social infrastructure, and information systems. An effects-based approach seeks to develop a commonly shared understanding of the operational environment to provide the commander with a more comprehensive picture of the challenges and the best balance of capabilities to shape the environment. The three main elements within an effects-based approach to operations are as follows:

1. Visualizing the operational environment beyond the traditional military battlespace as an interconnected system-of-systems comprised of friends, adversaries, and the unaligned.

2. Integrating military actions with those of other instruments of national power.
3. Assessing system behaviors and capabilities and effects attainment in addition to task accomplishment.

Maritime Power Projection

No one can predict with certainty the future security environment, but emerging trends require that the Navy focus on littorals and the land beyond. The Navy must remain expeditionary in nature, controlling the sea and moving around the globe to support U.S. national interests. The vision for the future is a Navy and Marine Corps team that will maintain a robust and credible forward presence. These forces provide a framework that complements other instruments of national power to build stability and favorably shape areas overseas. Forward presence, combined with knowledge superiority within the environment, will achieve the ultimate objective—maritime power projection—projecting U.S. power and influence from the sea, directly and decisively influencing events ashore.

Maritime Influence

Naval forces deployed or stationed in areas overseas demonstrate our national resolve, strengthen alliances, and dissuade potential adversaries. IO provides significant support to maritime influence operations during the phases of planning and assessment. U.S. naval forces will protect and use information to influence adversaries, advance friendly objectives, and shape the operating environment to our advantage. With an effects based approach to operations, maritime influence coordinates the employment of maritime activities to affect the attitudes and behaviors of an intended audience in support of commander objectives. With the goal of advancing U.S. interests, maritime influence activities may include actions to deter adversaries, reassuring allies and friends, sending signals of U.S. interest, and fostering good will.

Target Development

Warfighters win engagements and wars when the adversary makes a decision—based on knowledge derived from true or perceived information—to surrender due to an inability to obtain desired objectives. A comprehensive assessment of the adversaries and friendly abilities and functions within the operational environment provide the first step into developing targets. Friendly forces design all campaign plans to influence the adversary to make such a decision. The people and systems that comprise the information grids filter and process the information upon which the commander bases decisions and therefore require defending as part of IO planning. Target development includes nodes that have an impact on the adversary decision making process, which may include command and control systems, communications and weapon systems, and other situation awareness tools.

Environment Awareness and Shaping

EAS describes the functions performed by organizations to ensure that, despite the wide range of nonlethal and lethal means at the disposal of adversaries or potential adversaries, friendly forces are consistently capable of conducting decisive operations and achieving desired results at a minimal loss to friendly forces. The commander uses EAS to identify, protect, and leverage critical information systems, emissions, transmissions, and operational indicators, to achieve and maintain information superiority. Environment awareness equates to knowledge of the operational environment. This knowledge, resulting from the fusion of key elements of information, allows the commander and staff to correctly anticipate future conditions, assess changing conditions, establish requirements and priorities, and exploit emerging opportunities, while mitigating the impact of unexpected adversary actions. Environment shaping is the conscious action of molding the environment to prevent conflicts or placing U.S. interests in a favorable position. It involves the continual process of developing, evaluating, and revising the force operational profile within the environment, providing all warfare commanders with critical planning and execution support to ensure that missions are conducted with the least risk to friendly assets.

FORCEnet

FORCEnet provides the operational construct and architectural framework for achieving information superiority by integrating warriors, sensors, networks, command and control, platforms and weapons into a distributed force. FORCEnet provides naval forces with increased operational awareness, while supporting maritime power projection, ensuring access to the littoral areas and deterring conflict through the employment of a network of sensors and communication devices that provide the Navy with real time, shared awareness in support of operational objectives. Networked distributed forces allow warriors to apply speed in information gathering and sharing, and the ability to convert information into knowledge, command, and timely application of effects.

Information Operations Organization Structure

- **Naval Network Warfare Command**

  Naval Network Warfare Command (NAVNETWARCOM) provides the Navy's central operational authority and type commander for IO in support of naval forces afloat and ashore. NAVNETWARCOM maintains responsibility for identifying, coordinating, and assessing the Navy's IO requirements and FORCEnet architecture development. As the functional component for IO under U.S. Strategic Command, NAVNETWARCOM is responsible for the Navy's strategic IO planning and operational support.

- **Navy Information Operations Command Norfolk**

  Navy Information Operations Command (NIOC) Norfolk, the Navy's Center of Excellence for IO, is responsible for providing operationally focused training; planning support and augmentation from the tactical to the strategic level; developing IO doctrine, tactics, techniques, and procedures; advocating requirements in support of future effects-based warfare; conducting experimentation for evaluating emerging or existing IO technologies and doctrine; providing and managing IO data for fleet operations. NIOC Norfolk operates under the operational and administrative control of NAVNETWARCOM, and has three subordinate commands: NIOC San Diego, NIOC Whidbey Island and Navy IO Detachment Groton.

- **Navy Cyber Defense Operations Command**

  The Navy Cyber Defense Operations Command (NCDOC) coordinates, monitors, and oversees the defense of Navy computer networks and systems, including telecommunications, and is responsible for accomplishing computer network defense (CND) missions as assigned by NAVNETWARCOM and Joint Task Force - Global Network Operations (JTF-GNO).

- **Navy Information Operations Command Suitland**

  Navy Information Operations Command (NIOC) Suitland serves as Navy's IO innovation center and functions as the principal technical agent for research and development of prototype IO capabilities. NIOC Suitland supports the development capabilities encompassing all aspects of IO attack, protect, and exploit; maintaining an aggressive program to acquire and analyze state-of-the-art technologies (software and hardware), evaluate fleet applicability, and prototype developmental capabilities. NIOC Suitland maintains a collaborative relationship with Space and Naval Warfare Systems Command, Systems Center San Diego to provide efficient and effective technical expertise in command, control, communications, computers, intelligence, surveillance, reconnaissance and information operations.

NIOC Suitland also supports development coordination between NAVNETWARCOM, OPNAV, NIOC Norfolk, systems commands, IO technology center, and the commercial industry.

Navy Information Operations Employment Concept

Sea Power 21 describes future naval operations that will use information superiority and dispersed, networked force capabilities to deliver effective offensive power, defensive assurance, and operational independence to joint force commanders. To support Sea Power 21, the Navy's focus is to integrate and align IO to support all levels of operations:

- At the strategic level, national leadership and regional commanders will use IO to achieve national/theater shaping and influencing objectives. Regional commanders will integrate Navy IO capabilities with other services, other U.S. government departments and agencies, and partner nations as part of their theater security cooperation plans (TSCP).
- At the operational level, IO supports campaign/major operational objectives by providing information superiority through shaping and controlling the information environment. At this level, the focus of IO is control of adversary lines of communication (logistics information, command and control, and related capabilities and activities) while protecting the friendly information environment.

- At the tactical level, Navy IO will make full use of the core capabilities to dominate the information environment for the commander. At this level, IO will be used to tactically influence adversaries or deny, destroy, or degrade systems critical to the adversary's conduct of operations.

Levels of Operations	Key Goals Include…	Objectives to Support Goals Include…	Application of Navy IO Include…	Impact of Navy IO…
Strategic (National and Theater) National Security Strategy National Guidance & Military Strategy Theater Strategy & Campaign Plans	Implementation of long-term national and theater shaping, and theater security cooperation plans (TSCPs).	Influence nations/potential adversaries/decision makers globally or in a specific region(s). Support diplomacy, stabilize regions, and assure allies. Deter war. Support intelligence preparation of the environment, and shape environment to U.S. advantage.	CCDR, MHQ, and JFMCC (when assigned), will use IO to support TSCPs through presence, coordination with public affairs, port calls, multination exercises, peace operations, and support to strategic communications.	Demonstrate that the U.S. is engaged in the region and can project power. Demonstrate that the U.S. military can project power anywhere in region. Prepare intelligence baseline for future ops. Shape positive perception of U.S. actions.
Operational Subordinate Campaign Plans Major Operations	Decisively defeat adversary ability to control forces.	Shape and control information environment. Use spectrum of IO core capabilities to conduct (or support) force application, deny adversary intelligence, surveillance, reconnaissance (ISR) and command, control, communications, computers (C4). Support information superiority. Protect friendly information environment and physical domain.	The / MHQ use IO in continuing strategic roles plus applying Navy IO capabilities and weapons to engage adversary C4 and ISR and PSYOP to influence adversary forces and populations. Directly support conduct of joint or maritime operations/power projection.	Support information superiority for the joint force commander. Control information environment and physical domain by influencing, disrupting, or corrupting adversarial human and automated decisionmaking.
Tactical Operational Orders and OPTASKS Battles Engagements	Strike Group commander effectively using forces to achieve commander's assigned tasks. Coordinated use of EW, PSYOP, MILDEC, CNO, OPSEC capabilities embedded in Navy forces.	Control tactical information environment and physical domain. Disrupt adversary operations. Undermine adversary ability and will to fight. Disrupt adversary C4, ISR and defensive systems. Protect the naval/joint battle force.	During initial phases of a campaign, Navy strike groups may have the preponderance of tactical IO assets. Strike Group commander via the IO warfare commander will use IO to support MHQ objectives, and other tactical operations.	Achieve/maintain decision superiority, control tactical information environment and physical domains, achieves operational objectives of the MHQ and tactical objectives of the strike group commander.

Figure 2. Operational Model

The following key organizational concepts are being implemented to affect the operational model summarized in Figure 2:

- **Maritime Headquarters IO Cell**

References: NTTP 3-32.1 Maritime Headquarters with Maritime Operations Center, NTTP 3-13.1 Theater and Campaign Information Operations Planning (April 2008)

The MHQ IO Cell contributes to the shaping of the environment to enable tactical units to successfully execute assigned tasks. The IO Cell coordinates with the other maritime headquarters staff cells (i.e. horizontally) and with the IO cells of the other components and other government agencies through the joint force commander's IO staff (i.e. vertically). The IO cell works with elements of both the current operations cell, the future operations (FOPS) cell, and the Plans cell. Emphasis has been placed on the flexibility and scalability of Navy maritime headquarters (MHQs) with maritime operations centers (MOC) designed to perform normal and routine operations. Fleet commanders will establish global

MHQ-MOC's to serve geographic areas of responsibility, and may have additional JFMCC responsibilities.

The MHQ-MOC performs the fleet management and command and control (C2) role at the Navy operational-level of command across the range of military operations (ROMO). More importantly, the MHQ-MOC performs the roles of planning, directing, monitoring and assessing the integration and synchronization of Joint Maritime Force operational missions as outlined in the Navy operating concept. The MHQ-MOC organizes staff roles and responsibilities by integrating warfighting functions (C2, intelligence, movement and maneuver, fires, sustainment, and protection) across staff functions. Thus, the assessment and long range planning functions are joined in a future plans center and short term planning is performed in the future operations and current operations cells of the operations center. A MHQ-MOC is able to integrate staff actions horizontally and vertically, simultaneously conducting service and joint operations through the MOC and the fleet management functions by leveraging specialized fleet management staff elements. The MHQ-MOC has the capability to fulfill various roles including Commander, Joint Task Force (CJTF), Joint Force Maritime component commander (JFMCC), and naval component commander (NCC). Both the MOC and fleet management elements of the staff are supported by a third component consisting of shared support elements that provide personnel, processes, and systems that affect operations and fleet management functions.

- **Strike Group Level - The IO Warfare Commander (IWC)**

The IO Warfare Commander (IWC) assigned to each strike group is responsible for the protection of assigned forces against hostile information, information systems, and electronic attacks, as well as hostile propaganda and deceptive techniques. The IWC maintains the tactical IO picture and is responsible to the force commander for establishing force posture for emissions control (EMCON), information conditions (INFOCON), spectrum management, and maintaining a favorable tactical situation (TACSIT). The IWC supports all force plans and evolutions, while coordinating with theater and joint task force (JTF) IO planners.

Last Updated: October 2009

Air Force Information Operations Doctrine

Key doctrinal documents:
AFDD 2–5, *Information Operations*, 11 January 2005
AFDD 2–5.1, *Electronic Warfare Operations*, 5 November 2002
AFDD 2–5.3, *Public Affairs Operations*, 24 June 2005

AFDDs are available at: https://www.doctrine.af.mil/ and http://afpubs.hq.af.mil.

Information below is valid as of November 2009. However, at the time of printing the Information Operations Primer for AY 10, the process is now taking place which may result in some Air Force Information Operations doctrinal changes. This section reflects the currently published doctrine.

Excerpts of Air Force Doctrine - AFDD 2-5

Forward

The Air Force recognizes the importance of gaining a superior information advantage—an advantage obtained through information operations (IO) fully integrated with air and space operations. Today, gaining and maintaining information superiority are critical tasks for commanders and vital elements of fully integrated kinetic and nonkinetic effects-based operations. Information operations are conducted across the range of military operations, from peace to war to reconstitution. To achieve information superiority, our understanding and practice of information operations have undergone a doctrinal evolution that streamlines the focus of IO to improve the focus on warfighting.

The new framework of information operations groups the capabilities of influence operations, electronic warfare operations, and network warfare operations according to effects achieved at the operational level. Each of these capabilities consists of separate and distinct subcapabilities that, when combined and integrated, can achieve effects greater than any single capability. Integrated Control Enablers (ICE) is a new term used to define what was formerly expressed as information-in-warfare, or IIW. As our understanding of IO has advanced we have come see that ICE are not IO, but rather the "gain and exploit" capabilities that are critical to all air, space, and information operations. This new framework reflects the interactive relationship found between the defend/attack and the gain/exploit capabilities in today's Air Force.

Foundational Doctrine Statements

Foundational doctrine statements are the basic principles and beliefs upon which AFDDs are built.

- Information operations (IO) are integral to all Air Force operations and may support, or be supported by, air and space operations.

- The thorough integration of kinetic and nonkinetic air, space, and information capabilities provides the Air Force with a comprehensive set of tools to meet military threats.

- The Air Force defines information superiority as the degree of dominance in the information domain which allows friendly forces the ability to collect, control, exploit, and defend information without effective opposition.

- Decision superiority is about improving our capability to observe, orient, decide, and act (OODA loop) faster and more effectively than the adversary. Decision superiority is a relationship between adversary and friendly OODA loop processes.

- The three IO capabilities—influence operations, electronic warfare operations, and network warfare operations—while separate and distinct, when linked, can achieve operationally important IO effects. Effective IO depends on current, accurate, and specialized integrated control enablers (ICE) to provide information from all available sources.

- Information operations conducted at the operational and tactical levels may be capable of creating effects at the strategic level and may require coordination with other national agencies.

- IO should be seamlessly integrated with the normal campaign planning and execution process. There may be campaign plans that rely primarily on the capabilities and effects an IO strategy can provide, but there should not be a separate IO campaign plan.

- IO applications span the spectrum of warfare with many of the IO capabilities applied outside of traditional conflict. IO may offer the greatest leverage in peace, pre-conflict, transition-to-conflict, and reconstitution.

- Air Force IO may be employed in non-crisis support or military operations other than war (MOOTW) such as humanitarian relief operations (HUMRO), noncombatant evacuation operations (NEO), or counterdrug support missions where Air Force elements are subject to asymmetric threats that could hinder operations or place forces at risk.

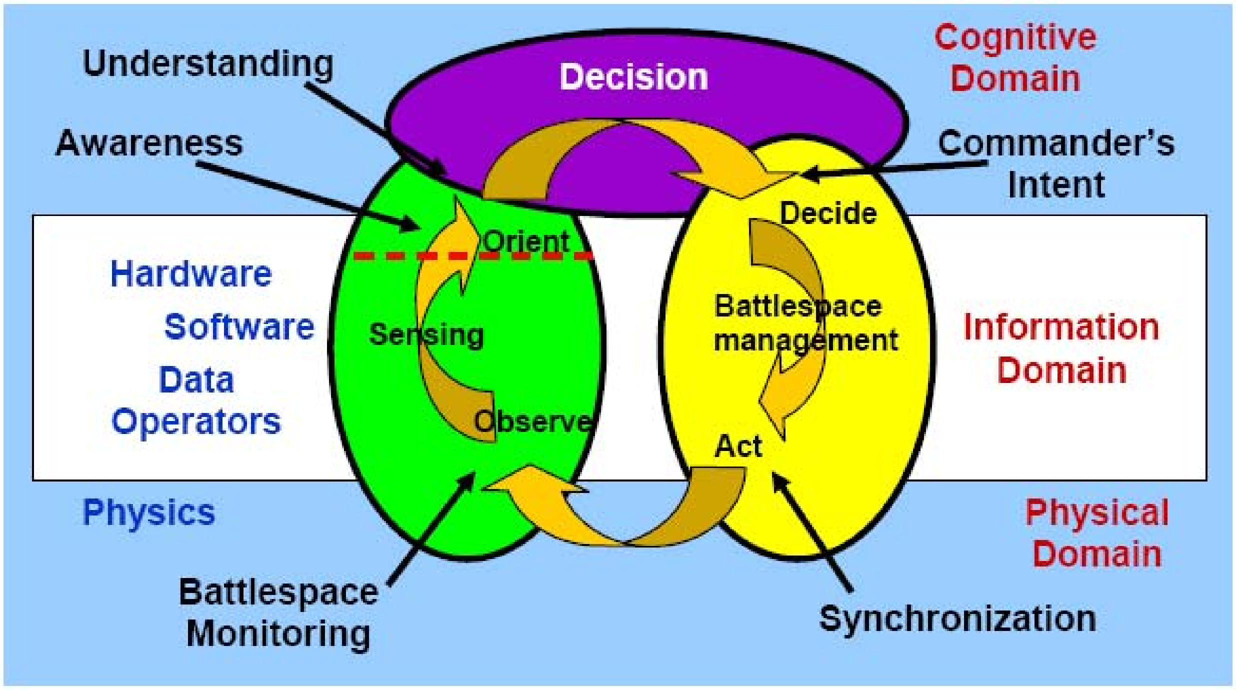
- IO presents additional challenges in effects-based planning as there are many variables. Many of these variables have human dimensions that are difficult to measure, may not be directly observable, and may also be difficult to acquire feedback.

1. The Nature of Information Operations

General Information operations (IO) are the integrated employment of the capabilities of influence operations, electronic warfare operations, and network warfare operations, in concert with specified integrated control enablers, to influence, disrupt, corrupt, or usurp adversarial human and automated decision making while protecting our own. Information operations provide predominantly nonkinetic capabilities to the warfighter. These capabilities can create effects across the entire battlespace and are conducted across the spectrum of conflict from peace to war and back to peace. Information superiority is a degree of dominance in the information domain which allows friendly forces the ability to collect, control, exploit, and defend information without effective opposition. Information superiority is a critical part of air and space superiority, which gives the commander freedom from attack, freedom to maneuver, and freedom to attack. Information operations (IO) are integral to all Air Force operations and may support, or be supported by, air and space operations. IO, therefore, must be integrated into air and space component operations in the same manner as traditional air and space capabilities.

Warfare in the Information Age Warfare in the information age has placed greater emphasis on influencing political and military leaders, as well as populations, to resolve conflict. Information technology (IT) has increased access to the means to directly influence the populations and its leaders. IT has distributed the process of collection, storage, dissemination, and processing of information. The Air Force goal is to leverage this technology to achieve air, space, and information superiority and to be able to operate in a faster decision cycle (decision superiority) than the adversary. Decision superiority is a competitive advantage, enabled by an ongoing situational awareness, that allows commanders and their forces to make better-informed decisions and implement them faster than their adversaries can react. Decision superiority is about improving our ability to observe, orient, decide, and act (OODA loop) faster and more effectively than the adversary. *Joint Vision 2020* describes it as "better decisions arrived at and implemented faster than an opponent can react, or in a non-combat situation, at a tempo that allows the force to shape the situation or react to changes and accomplish its mission." Decision superiority is a relationship between adversary and friendly OODA loop processes. Decision superiority is more likely to be achieved if we plan and protect our OODA loop processes in conjunction with analyzing, influencing, and attacking the adversary's.

The Information Environment [The information environment can be modeled as the interaction of the physical, information, and cognitive domains as shown below.]



This model provides a means to understand the IO environment. It also provides a logical foundation for the IO capabilities of influence operations, network warfare operations, and electronic warfare operations. All activities in the physical environment have effects in the cognitive environment. Electronic warfare operates in the electromagnetic spectrum, although it creates effects across the range of the IO operating environment. Network warfare operations are focused on the information domain, which is composed of a dynamic combination of hardware, software, data, and human components. Influence operations are focused on affecting the perceptions and behaviors of leaders, groups, or entire populations. The means of influencing can be physical, informational, or both. The cognitive domain is composed of separate minds and personalities and is influenced by societal norms, thus the cognitive domain is neither homogeneous nor continuous.

Societies and militaries are striving to network this "information domain" with the objective of shortening the time it takes for this distributed observe, orient, decide, and act process to occur. It also allows us to automate certain decision processes and to build multiple decision models operating simultaneously. In essence, the information domain continues to expand. New technology increases our society's ability to transfer information as well as an adversary's opportunity to affect that information. Information operations are not focused on making decision loops work; IO focuses on defending our decision loops and influencing or affecting the adversary's decisions loops. This integration of influence, network warfare, and electronic warfare operations to create effects on OODA loops is the unifying theme of IO. Whether the target is national leadership, military C2, or an automated industrial process, how the OODA process is implemented provides both opportunities and vulnerabilities.

The three IO capabilities—influence operations, electronic warfare operations, and network warfare operations—while separate and distinct, when linked, can achieve operationally important IO effects. In addition, effective IO depends on current, accurate, and specialized integrated control enablers (ICE) to provide information from all available sources. The thorough integration of kinetic and nonkinetic air, space, and information capabilities provides the Air Force with a comprehensive set of tools to meet military threats.

Influence Operations Influence operations are focused on affecting the perceptions and behaviors of leaders, groups, or entire populations. Influence operations employ capabilities to affect behaviors, protect operations, communicate commander's intent, and project accurate information to achieve desired effects across the cognitive domain. These effects should result in differing behavior or a change in the adversary's decision cycle, which aligns with the commander's objectives. The military capabilities of influence operations are psychological operations (PSYOP), military deception (MILDEC), operations security (OPSEC), counterintelligence (CI) operations, counterpropaganda operations and public affairs (PA) operations. Public affairs, while a component of influence operations, is predicated on its ability to project truthful information to a variety of audiences.

Network Warfare Operations Network warfare operations are the integrated planning, employment, and assessment of military capabilities to achieve desired effects across the interconnected analog and digital network portion of the battlespace. Network warfare operations are conducted in the information domain through the combination of hardware, software, data, and human interaction. Networks in this context are defined as any collection of systems transmitting information. Examples include, but are not limited to, radio nets, satellite links, tactical digital information links (TADIL), telemetry, digital track files, telecommunications, and wireless communications networks and systems. The operational activities of network warfare operations are network attack (NetA), network defense (NetD) and network warfare support (NS).

Electronic Warfare Operations Electronic warfare operations are the integrated planning, employment, and assessment of military capabilities to achieve desired effects across the electromagnetic domain in support of operational objectives. Electronic warfare operates across the electromagnetic spectrum, including radio, visible, infrared, microwave, directed energy, and all other frequencies. It is responsible for coordination and deconfliction of all friendly uses of the spectrum (air, land, sea, and space) as well as attacking and denying enemy uses. For this reason it is a historically important coordinating element in all operations, especially as current and future friendly uses of the electromagnetic spectrum multiply. The military capabilities of electronic warfare operations are electronic attack, electronic protection, and electronic warfare support.

Integrated Control Enablers Information operations, like air and space operations, are reliant on the integrated control enablers (ICE). ICE includes intelligence, surveillance, and reconnaissance (ISR), network operations (NetOps), predictive battlespace awareness (PBA), and precision navigation and timing (PNT). Information operations are highly dynamic and maneuverable. The transition between the find, fix, track, target, engage, and assess (F2T2EA) phases can be nearly instantaneous. The ICE components support this interactive relationship and strive to provide commanders continuous decision-quality information to successfully employ information operations.

2 – Influence Operations

General Influence operations are employment of capabilities to affect behaviors, protect operations, communicate commander's intent, and project accurate information to achieve desired effects across the cognitive domain. These effects should result in differing behavior or a change in the adversary decision cycle, which aligns with the commander's objectives. They should influence adversary decision-making, communicate the military perspective, manage perceptions, and promote behaviors conducive to friendly objectives. Counterpropaganda operations, psychological operations (PSYOP), military deception (MILDEC), operations security (OPSEC), counterintelligence (CI) operations, and public affairs (PA) operations are the military capabilities of influence operations. They support the commander's objectives and support the Air Force in achieving air, space, and information superiority. This is accomplished by conveying selected information and indicators to target audiences; shaping the perceptions of target decision-makers; securing critical friendly information; protecting against espionage, sabotage, and other intelligence gathering activities; and communicating unclassified information about friendly activities to the global audience.

Psychological Operations Focused on the cognitive domain of the battlespace, PSYOP targets the mind of the adversary. In general, PSYOP seeks to induce, influence, or reinforce the perceptions, attitudes, reasoning, and behavior of foreign leaders, groups, and organizations in a manner favorable to friendly national and military objectives. PSYOP supports these objectives through the calculated use of air, space, and IO with special emphasis on psychological effects-based targeting.

Military Deception Military deception (MILDEC) capabilities are a powerful tool in military operations and should be considered throughout the operational planning process. Military deception misleads or manages the perception of adversaries, causing them to act in accordance with friendly objectives.

Operations Security Operations security (OPSEC) is an activity that helps prevent our adversaries from gaining and exploiting critical information. OPSEC is not a collection of specific rules and instructions that can be applied to every operation, it is a methodology that can be applied to any operation or activity for the purpose of denying critical information to the adversary. Critical information consists of information and indicators that are sensitive, but unclassified. OPSEC aims to identify any unclassified activity or information that, when analyzed with other activities and information, can reveal protected and important friendly operations, information, or activities.

Counterintelligence The Air Force Office of Special Investigations (AFOSI) initiates, conducts, and/or oversees all Air Force counterintelligence (CI) investigations, activities, operations, collections, and other related CI capabilities. Counterintelligence is defined as information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities. AFOSI supports influence operations through CI operations designed to detect, destroy, neutralize, exploit, or prevent espionage activities through identification, manipulation, deception, or repression of the adversary.

Public Affairs Operations Commanders conduct PA operations to assess the information environment in areas such as public opinion and to recognize political, social, and cultural shifts. Public affairs operations are a key component of informational flexible deterrent options and build commanders' predictive awareness of the international public information environment and the means to use information to take offensive and preemptive defensive actions in Air Force operations. Public affairs operations are the lead activity and the first line of defense against adversary propaganda and disinformation. Falsehoods are easily identified when the truth is well known. [Public affairs operations are accomplished through] four core tasks: media operations, internal information, community relations, and strategic communication planning.

Counterpropaganda Operations The Air Force defines counterpropaganda operations as activities to identify and counter adversary propaganda and expose adversary attempts to influence friendly populations and military forces situational understanding. They involve those efforts to negate, neutralize, diminish the effects of, or gain an advantage from foreign psychological operations or propaganda efforts.

Supporting Activities Influence operations are most successful through the seamless integration of kinetic and nonkinetic capabilities. Influence operations may be supported and enhanced by physical attack to create or alter adversary perceptions. Influence operations require support from many Air Force capabilities to include tailored ISR, combat camera operations, and cultural expertise.

3 – Network Warfare Operations

Network warfare operations (NW Ops) are the integration of the military capabilities of network attack (NetA), network defense (NetD), and network warfare support (NS). The integrated planning and employment of network warfare operations along with electronic warfare operations (EW Ops), influence operations, and other military capabilities are conducted to achieve desired effects across the information domain.

Network Attack Network attack (NetA) is employment of network-based capabilities to destroy, disrupt, corrupt, or usurp information resident in or transiting through networks. Networks include telephony and data services networks. Additionally, NetA can be used to deny, delay, or degrade information resident in networks, processes dependent on those networks, or the networks themselves. A primary effect is to influence the adversary commander’s decisions.

Network Defense Network defense (NetD) is employment of network-based capabilities to defend friendly information resident in or transiting through networks against adversary efforts to destroy, disrupt, corrupt, or usurp it. NetD can be viewed as planning, directing, and executing actions to prevent unauthorized activity in defense of Air Force information systems and networks and for planning, directing, and executing responses to recover from unauthorized activity should it occur.

Network Warfare Support Network warfare support (NS) is the collection and production of network related data for immediate decisions involving NW Ops. NS is critical to NetA and NetD actions to find, fix, track, and assess both adversaries and friendly sources of access and vulnerability for the purpose of immediate defense, threat prediction and recognition, targeting, access and technique development, planning, and execution in NW Ops.

4 – Electronic Warfare Operations

General Electronic warfare (EW) is any military action involving the use of electromagnetic or directed energy to manipulate the electromagnetic spectrum or to attack an adversary. The Air Force describes electronic warfare operations (EW Ops) as the integrated planning, employment, and assessment of military capabilities to achieve desired effects across the electromagnetic domain in support of operational objectives. The EW spectrum is not merely limited to radio frequencies but also includes optical and infrared regions as well. EW assists air and space forces to gain access and operate without prohibitive interference from adversary systems, and actively destroys, degrades, or denies opponents’ capabilities, which would otherwise grant them operational benefits from the use of the electromagnetic spectrum.

Electronic Warfare Operations EW is a key contributor to air superiority, space superiority, and information superiority. The most important aspect of the relationship of EW to air, space, and information operations is that EW enhances and supports all operations throughout the full spectrum of conflict. Air Force EW resources and assets may take on new roles in support of operations as the electronic warfare operation mission evolves. The three military capabilities of EW operations are electronic attack (EA), electronic protection (EP), and electronic warfare support (ES). All three contribute to air and space operations, including the integrated IO effort. Control of the electromagnetic spectrum is gained by protecting friendly systems and countering adversary systems.

Electronic attack (EA) is the division involving the use of electromagnetic, directed energy (DE), or anti-radiation weapons to attack personnel, facilities, or equipment with the intent of deceiving, disrupting, denying, and/or destroying adversary combat capability. It also deceives and disrupts the enemy integrated air defense system (IADS) and communications, as well as enables the destruction of these adversary capabilities via lethal strike assets.

Electronic protection (EP) enhances the use of the electronic spectrum for friendly forces. Electronic protection is primarily the defensive aspect of EW that is focused on protecting personnel, facilities, and equipment from any effects of friendly or adversary employment of electronic warfare that degrade, neutralize, or destroy friendly combat capability.

Electronic warfare support (ES), the collection of electromagnetic data for immediate tactical applications (e.g., threat avoidance, route selection, targeting, or homing) provides information required for timely decisions involving electronic warfare operations.

5 – Information Operations Planning and Execution

Information operations are integral to military operations and are a prerequisite for information superiority. IO supports, and may also be supported by, air and space operations and needs to be planned and executed just like air operations. IO should be seamlessly integrated with the normal campaign planning and execution process. There may be campaign plans that rely primarily on the capabilities and effects an IO strategy can provide, but there should not be a separate IO campaign plan.

One of the commander's priorities is to achieve decision superiority over an adversary by gaining information superiority and controlling the information environment. This goal does not in any way diminish the commander's need to achieve air and space superiority but rather facilitates efforts in those areas and vice versa. The aim of information superiority is to have greater situational awareness and control than the adversary. Effective use of IO leads to information superiority. The effort to achieve information superiority depends upon two fundamental components: an effects-based approach, and well-integrated IO planning and execution accomplished by IO organizations.

Effects-Based Approach The ability to create the effects necessary to achieve campaign objectives, whether at the strategic, operational, or tactical levels, is fundamental to the success of the Air Force. An effect is the anticipated outcome or consequence that results from a particular military operation. The emphasis on effects is as crucial for successful IO as for any other air and space power function. Commanders should clearly articulate the objectives or goals of a given military operation. Effects should then flow from objectives as a product of the military operations designed to help achieve those objectives. Based on clear objectives, planners should design specific operations to achieve a desired outcome, and then identify the optimum capability for achieving that outcome. It is important to realize that operational assessment may be more challenging in IO because the effects are often difficult to measure. IO may also be based upon common sense, a rule of thumb, simplification, or an educated guess that reduces or limits the search for solutions in domains that are difficult or poorly understood. For example, psychological effects are not only difficult to measure; they may also not manifest themselves until later in time. There are also second-order and third-order effects that should be taken into consideration, and again, these may not manifest themselves until much later. IO presents additional challenges in effects-based planning as there are many variables. Many of these variables also have human dimensions that are difficult to measure, may not be directly observable, and may also be difficult to acquire feedback. At all times, objectives must be set and effects must be analyzed from the point of view of the culture where operations are being conducted.

Information Operations Organizations A number of Air Force organizations contribute to effective IO. The following discuss several of the key organizations employed in information operations.

Information Warfare Flight (IWF) IO can be conducted throughout the spectrum of peace and conflict. In peacetime, the major command/ numbered air force (MAJCOM/NAF) IWF is the operational planning element for IO and may coordinate IO actions when an air and space operations center (AOC) has not been activated. When the AOC is activated, a portion of the IWF is established as an IO team and integrates into the warfighting divisions within the AOC (Strategy, Plans, ISR, Combat Operations, etc.). The IO team provides the IO expertise to plan, employ, and assess IO capabilities prior to the initiation of hostilities, transition to conflict, and reconstitution.

EW Ops Organizations Electronic warfare is conducted by units with capabilities ranging across the electronic attack, protect, and support functions. EW operations require attention before, during, and after military operations. A joint EW coordination cell (EWCC) is the necessary planning and execution organization to orchestrate the activities of units to achieve EW objectives of the campaign plan.

Network Defense and Network Operations Organizations NetD and NetOps organizations provide the JFC with critical capabilities to realize the effects of information and decision superiority. Collectively, these organizations provide varying degrees of NetD and NetOps support. They provide commanders with real-time intrusion detection and perimeter defense capabilities, network management and fault resolution activities, data fusion, assessment, and decisions support. During employment, the organizations are arranged into a three-tiered operational hierarchy, which facilitates synchronized application of their collective capabilities in support of the DOD's defense-in-depth security strategy.

6 – Integrated Control Enablers

Information operations are dependent on [integrated control enablers] (ICE). The integrated control enablers are critical capabilities required to execute successful air, space, and information operations and produce integrated effects for the joint fight. These include intelligence, surveillance, and reconnaissance (ISR), network operations (NetOps), predictive battlespace awareness (PBA), and precision navigation and timing (PNT).

Network Operations and Information Assurance NetOps encompasses information assurance (IA), system and network management, and information dissemination management. The Air Force and joint community have come to recognize these pillars as information assurance and network defense, enterprise service management/network management, and content staging/information dissemination management respectively. NetOps consists of organizations, procedures, and functionalities required to plan, administer, and monitor Air Force networks in support of operations and also to respond to threats, outages, and other operational impacts.

Information assurance (IA) comprises those measures taken to protect and defend information and information systems by ensuring their availability, integrity, authenticity, confidentiality, and non-repudiation (ability to prove sender’s identity and prove delivery to recipient). IA spans the full lifecycle of information and information systems. IA depends on the continuous integration of trained personnel, operational and technical capabilities, and necessary policies and procedures to guarantee continuous and dependable information, while providing the means to efficiently reconstitute these vital services following disruptions of any kind, whether from an attack, natural disaster, equipment failure, or operator error. In an assured information environment, warfighters can leverage the power of the information age.

Intelligence, Surveillance, and Reconnaissance ISR is the integrated capabilities to task, collect, process, exploit, and disseminate accurate and timely intelligence information. ISR is a critical function that helps provide the commander the situational and battlespace awareness necessary to successfully plan and conduct operations. Commanders use the intelligence information derived from ISR assets to maximize their own forces' effectiveness by optimizing friendly force strengths, exploiting adversary weaknesses, and countering adversary strengths.

Predictive Battlespace Awareness Effective IO depends upon a successful PBA. As a maturing concept, PBA is "knowledge of the operational environment that allows the commander and staff to correctly anticipate future conditions, assess changing conditions, establish priorities, and exploit emerging opportunities while mitigating the impact of unexpected adversary actions" (Air Force Pamphlet 14-118). In order to accomplish this, PBA lays out a methodology that enables integration of all intelligence, surveillance, and reconnaissance assets available to commanders, in order to maximize their ability to predict enemy courses of action and decide friendly courses of action. One of the first steps in PBA is assessing friendly vulnerabilities and adversary strengths and weaknesses in order to predict enemy courses of action through IPB. This level of awareness requires development and integration of five key activities: IPB, target development, ISR strategy and planning, ISR employment, and assessment. These activities are continuously refined in parallel to provide a seamless understanding of the battlespace.

Precision Navigation and Timing Precision navigation and timing (PNT) provided by space-based systems are essential to IO by providing the ability to integrate and coordinate IO force application to create effects across the battlespace.

7 – Education and Training

Education and training provide the foundation for conducting effective information operations. All Airmen should have a general understanding of information operations capabilities. As in other specialties, IO personnel should be thoroughly trained in the specific IO processes that relate to their particular field of expertise. IO personnel should recognize the contribution their functional specialty makes to the warfighter to help achieve the goal of information superiority. The intent of IO education and training is to ensure Air Force IO operators clearly understand the principles, concepts, and characteristics of information operations. Finally, while not every Airman needs a comprehensive course in information operations, every Airman should understand that IO is a key function of the Air Force distinctive capabilities of information superiority and air and space superiority.

Note: End of AFDD 2-5 extract.

Last Updated: November 2009

This Page Intentionally Blank

Service Component Information Operations Organizations

OPERATIONS
1ST
INFORMATION
COMMAND
(LAND)

ARMY RESERVE INFORMATION OPERATIONS COMMAND
I
O
Guardians of the Net
IIIII010001

MARINE CORPS
VERAX INDICIUM MOVET ANIMUM
INFORMATION OPERATIONS CENTER

UNITED STATES
NAVY

AIR FORCE ISR AGENCY

24
TWENTY-FOURTH AIR FORCE

LUX EX TENEBRIS

688TH INFORMATION OPERATIONS WING

689TH COMBAT COMMUNICATIONS WING

This Page Intentionally Blank

Army – 1st Information Operations Command (1st IO Cmd)

Mission: 1st Information Operations (IO) Command (Land) provides IO support to the Army and other Military Forces through deployable IO support teams, IO reachback planning and analysis, and the synchronization and conduct of Army Computer Network Operations (CNO) in coordination with other CNO and Network Operations stakeholders, to operationally integrate IO, reinforce forward IO capabilities, and to defend Cyberspace in order to enable IO throughout the Information Environment.

Tasks:

1. Organize, train, equip and deploy mission capable IO Support Teams to provide IO planning and execution support or to conduct IO assessments as directed.

2. Provide IO planning plus operational, technical, and intelligence analysis reachback support to deployed IO support teams and supported commands.

3. Provide IO training support to LCCs, Army Commands, other Service Commands, Joint Forces, Agencies and Activities, as directed

4. Execute the Army Reprogramming Analysis Team-Threat Analysis program.

5. Develop and promote processes and procedures to ensure IO interoperability with Joint Forces, other Services, Inter-agencies, and Allies.

6. Provide IO support for the assessment of force readiness and capabilities of Land Component Forces to accomplish their assigned missions as directed.

7. Synchronize and conduct Army Computer Network Operations (CNO) in coordination with CNO and NETOPS stakeholders to defend Cyberspace and to enable other Information Operations as directed.

8. Operate and maintain the Army's Operations Security (OPSEC) Support Element.

9. Act as the Functional Proponent for Military Deception.

As the single Army organization dedicated to IO, 1st IO Cmd is responsible for providing IO support to the warfighter in planning, synchronizing, de-conflicting, executing, and assessing IO. The Command supports warfighting and other commanders in conflict, other contingency operations, garrison, and in field training exercises and experiments. 1st IO Cmd operates with and across each of the IO competencies to gain an advantage through coordinated use of multiple capabilities to affect the Information Environment. 1st IO Cmd deploys IO Support Teams that provide IO planning, vulnerability assessments, OPSEC awareness, training, and technical support for computer incidents and intrusions. 1st

IO Cmd conducts and synchronizes operations across the computer network operations (CNO) spectrum in the defense of Army networks by conducting continuous Computer Network Defense (CND) operations and CND-Response Actions in coordination with computer network service providers. Additionally, 1st IO Cmd provides IO reachback capability to deployed teams and to the operational and tactical staffs of deployed forces, as directed. Lastly, 1st IO Cmd executes the Army Reprogramming Analysis Team-Threat Analysis program to enhance the survivability and lethality of warfighting systems. These skilled professionals offer commanders nontraditional options for today's technologically advanced battlespace.

Subordination: 1st IO Cmd is a major subordinate command to the U.S. Army Intelligence and Security Command (INSCOM) but is under the Operational Control and tasking of the Army G-3/5/7 (Director of Operations, Readiness and Mobilization).

Leadership: The Commander of 1st IO Cmd is an Army Colonel who is qualified as a functional Area 30, Information Operations Officer.

Location: The 1st IO Cmd is located at Ft. Belvoir, VA within the INSCOM HQs building. 1st IO Cmd has liaison positions established at the Pentagon, NSA, JFCC-NW, CAC, USAIOP/EWP, Joint Information Operations Warfare Center/Air Force IO Command, US Army Special Operations Command at Fort Bragg, USCENTCOM, and the National Air and Space Intelligence Center. 1st IO Cmd has six Regional Computer Emergency Response Teams (RCERTs) that are collocated with each of the Army Service Component Commands.

https://www.1stiocmd.army.mil/io_portal/Public/Pages/Public_Main.cfm (Requires current CAC card for access.)

Last Updated: September 2009

Army Reserve Information Operations Command (ARIOC)

Mission: The Army Reserve Information Operations Command (ARIOC) conducts Computer Network Operations (CNO) and Information Operations (IO) to support full spectrum Army and Joint Warfighting operations.

Tasks:

- Organize, train, equip and deploy mission capable CNO Support Teams to conduct planning, intelligence support and analysis, synchronization, and integration of Army CNO capabilities into full spectrum operations. ARIOC conducts cyber counter-reconnaissance, cyber-strategic reconnaissance, incident handling & response, and computer defense and assistance program (CDAP) augmentation in support of the 1st IOC (L) Army Computer Emergency Response Team (ACERT) and Regional Computer Emergency Response Team (RCERT) SWA mission. The command monitors the Defense Research and Engineering Network (DREN), deploys Vulnerability Assessment Teams (VAT), and supports the Army Net Risk Assessment Mission.

- Operates the secure, stand-alone ARIOC Cyber range. This network is used for CNO analysis, doctrine development, exercise support, training, certification and validation of cyber warrior skill sets. This network facilitates ARIOC participation in Joint level exercises with the JFCOM Joint IO Range.

- Develops, promotes policies, procedures and processes to integrate IO into operations of the Army Reserve, reserve components of other services, inter-agencies and allies.

- Organize, train, equip and deploy mission capable IO Field Support Teams (FST) to conduct planning, integration and assessment of IO in support of full spectrum operations. ARIOC conducts IO FST missions in support of CJTF-101 and individual augmentation of MNF-I mission.

The Army Reserve IO Command (ARIOC) applies the civilian acquired IT skills, knowledge and abilities of its citizen-soldiers to support Army and Joint Cyberspace requirements of the 21st century. ARIOC deploys experienced, skilled IO teams and individuals to augment Army & Joint capabilities in full spectrum operations.

Subordination: The ARIOC is a subordinate unit of the U.S. Army Reserve Readiness Command (USARRC), Fort Jackson, SC. ARIOC receives its operational tasking through the Army G-3 (Director of Operations, Readiness and Mobilization) and Forces Command (FORSCOM).

Leadership: The Commander of the ARIOC is an Army Reserve Colonel (O-6).

Location: ARIOC HQ is in Adelphi, MD at the Army Research Lab, Phone: S3 - 301.394.1144 or DSN 290-1144, DCDR - 301.394.1190 or DSN 290-1190.

Last Updated October 2009.

This Page Intentionally Blank

United States Army Information Proponent Office (ARIOC)

The U.S. Army Information Proponent Office (USAIPO) **is charged to develop the capabilities and capacity across Army Doctrine, Organizations, Training and Education, Materials, Leadership, Personnel, and Facilities (DOTMLPF) that leverage the power of information to achieve mission success across the full range of military operations.**

As the U.S. Army Proponent Chief, the Commanding General, US Army Combined Arms Center (CG, CAC) established the IPO as a directorate within CAC Capabilities Development Integration Directorate to serve as his executive agent for accomplishing this critical mission. The major responsibilities of IPO are derived from CG, CAC's and CDID's priorities.

Mission of High Headquarters

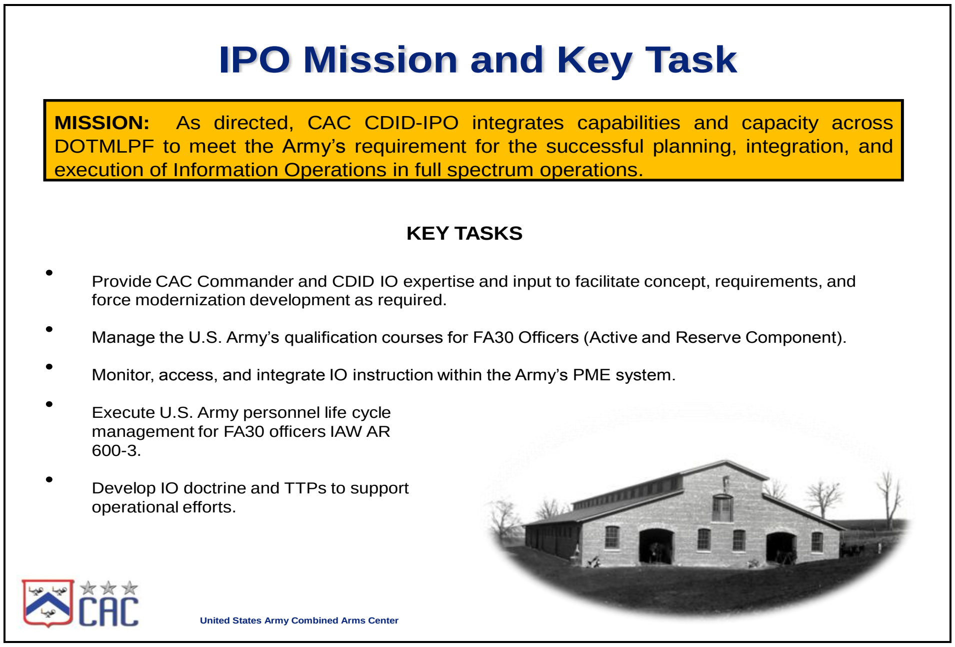
CAC Mission: Provides leadership and supervision for the leader development and profession military and civilian education, institutional and collective training, functional training, training support, doctrine, lessons learned, battle command, and specified areas designated by CG, TRADOC.

CAC-CDID MISSION: conducts **capability development and integration** for battle command, division headquarters and above, force management requirements in the Modular Force, information operations and cyberspace. The organization develops concepts, defines requirements, and conducts experiments in order to validate DOTMLPF-integrated combined arms capabilities that complement joint, interagency, and multinational capabilities. CAC-CDID performs other integration tasks as assigned within the scope of CAC's core functions, major responsibilities, and proponencies.

United States Army Combined Arms Center

2

a. USAIPO mission and key tasks vision were approved by Director CDID in October 2009.



IPO Mission and Key Task

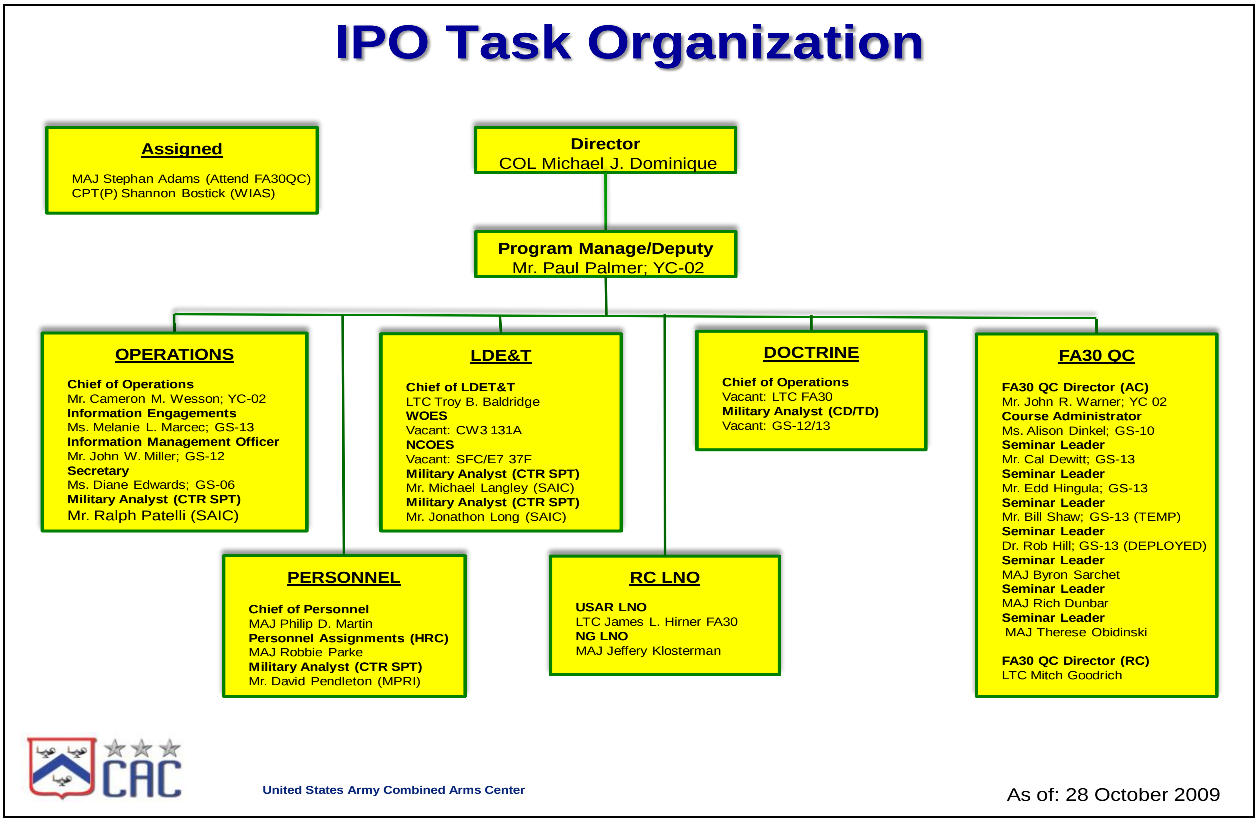
MISSION: As directed, CAC CDID-IPO integrates capabilities and capacity across DOTMLPF to meet the Army's requirement for the successful planning, integration, and execution of Information Operations in full spectrum operations.

KEY TASKS

- Provide CAC Commander and CDID IO expertise and input to facilitate concept, requirements, and force modernization development as required.
- Manage the U.S. Army's qualification courses for FA30 Officers (Active and Reserve Component).
- Monitor, access, and integrate IO instruction within the Army's PME system.
- Execute U.S. Army personnel life cycle management for FA30 officers IAW AR 600-3.
- Develop IO doctrine and TTPs to support operational efforts.

CAC United States Army Combined Arms Center

b. USAIP0 is organized as follows to accomplish this mission:



IPO Task Organization

Assigned
MAJ Stephan Adams (Attend FA30QC)
CPT(P) Shannon Bostick (WIAS)

Director
COL Michael J. Dominique

Program Manage/Deputy
Mr. Paul Palmer; YC-02

OPERATIONS
Chief of Operations
Mr. Cameron M. Wesson; YC-02
Information Engagements
Ms. Melanie L. Marcec; GS-13
Information Management Officer
Mr. John W. Miller; GS-12
Secretary
Ms. Diane Edwards; GS-06
Military Analyst (CTR SPT)
Mr. Ralph Patelli (SAIC)

LDE&T
Chief of LDET&T
LTC Troy B. Baldridge
WOES
Vacant: CW3 131A
NCOES
Vacant: SFC/E7 37F
Military Analyst (CTR SPT)
Mr. Michael Langley (SAIC)
Military Analyst (CTR SPT)
Mr. Jonathon Long (SAIC)

DOCTRINE
Chief of Operations
Vacant: LTC FA30
Military Analyst (CD/TD)
Vacant: GS-12/13

FA30 QC
FA30 QC Director (AC)
Mr. John R. Warner; YC 02
Course Administrator
Ms. Alison Dinkel; GS-10
Seminar Leader
Mr. Cal Dewitt; GS-13
Seminar Leader
Mr. Edd Hingula; GS-13
Seminar Leader
Mr. Bill Shaw; GS-13 (TEMP)
Seminar Leader
Dr. Rob Hill; GS-13 (DEPLOYED)
Seminar Leader
MAJ Byron Sarchet
Seminar Leader
MAJ Rich Dunbar
Seminar Leader
MAJ Therese Obidinski

FA30 QC Director (RC)
LTC Mitch Goodrich

PERSONNEL
Chief of Personnel
MAJ Philip D. Martin
Personnel Assignments (HRC)
MAJ Robbie Parke
Military Analyst (CTR SPT)
Mr. David Pendleton (MPRI)

RC LNO
USAR LNO
LTC James L. Hirner FA30
NG LNO
MAJ Jeffery Klosterman

CAC United States Army Combined Arms Center

As of: 28 October 2009

c. Public Website: http://usacac.army.mil/cac2/IPO/index.asp

Last Updated: October 2009

Marine Corps Information Operations Center

Mission: The Marine Corps Information Operations Center will provide Marine Air-Ground Task Force (MAGTF) commanders and the Marine Corps a responsive and effective full-spectrum IO planning and PSYOP delivery capability by means of deployable support teams and a comprehensive general support IO reach-back capability IOT support the integration of IO into Marine Corps operations.

Marine Corps IO Center Support to the MAGTF:

1. Provides mobile training teams (MTT) for on-site unit and MAGTF IO training.

2. Supports unit and MAGTF IO officers/staff during exercises with the integration of IO into the Marine Corps Planning Process (MCPP).

3. Deploys IO subject matter experts (SMEs) to assist with the integration of IO during pre-deployment training cycles.

4. Provides reach-back/coordination to the MAGTF throughout operational deployments.

5. Provides deployed IO mission planners as required, to augment the MAGTF's organic IO capabilities during operational deployments.

6. Coordinates external (USMC, Joint, Interagency, Coalition, and OGA) IO capabilities of the MAGTF as required.

Established July 15, 2009, the Marine Corps IO Center is the Marine Corps' executive agent for the Marine Corps IO Program (MCO 3120.10) and the centralized repository of USMC IO expertise. The Marine Corps IO Center will ensure the establishment of IO capabilities throughout the Marine Corps, integrate IO into Marine Corps Operating Concepts, and directly support Marine Forces during all phases of operations by providing training, mission planning, reach-back support, and coordination of USMC, Joint, Coalition and Interagency capabilities. Additionally, the MCIOC will augment the deployed MAGTF with scalable, mission-tailored IO planning teams during contingency operations which require support that exceeds the MAGTF's organic IO capabilities.

Upon full operational capability (January 2011), the IO Center will maintain:

- Four IO Planning Teams (IOPT) and four Expeditionary PSYOP Teams (EPT), task organized and deployable, to support exercises, pre-deployment training programs (PTP), and deploying MAGTFs

- Two Direct Support (DS) reach-back cells to support deployed IOPTs, EPTs and MAGTF staffs

- One General Support (GS) reach-back cell to support Marine Corps units, other services when able, and interagency integration.

Subordination: The Marine Corps IO Center is subordinate to Deputy Commandant for Plans, Policies and Operations (DC, PP&O). IOPTs and EPTs will, in most cases, be attached to supported MAGTFs during operational deployments, including pre-deployment exercises.

Leadership: The Director of the IO Center is a Colonel (O-6).

Location: The IO Center is located aboard Marine Corps Base Quantico, Virginia.

For more information contact Capt Shawn M. Mercer at 703-784-5115 or shawn.m.mercer@usmc.mil.

Updated: October 2009

Navy Information Operations Organizations

- **This section presents brief descriptions of selected U.S. Navy Information Operations organizations.**
-
- The planned revision to NWP 3-13 Navy Information Operations have been placed on hold awaiting JP 3-13 ongoing revisions.
- The effects of the establishment of JOINT CYBER COMMAND and the supporting FLEET CYBER COMMAND are not currently reflected in Navy IO TTP and CONOPS and are not addressed in this summary
- When NWP 3-13 is completed the new document can be found at http://www.nwdc.navy.smil.mil under the Navy Doctrine Library System link.

- **Naval Network Warfare Command**

  Naval Network Warfare Command (NAVNETWARCOM) provides the Navy's central operational authority and type commander for IO in support of naval forces afloat and ashore. NAVNETWARCOM maintains responsibility for identifying, coordinating, and assessing the Navy's IO requirements and FORCEnet architecture development. As the functional component for IO under U.S. Strategic Command, NAVNETWARCOM is responsible for the Navy's strategic IO planning and operational support.

- **Navy Information Operations Command Norfolk**

  Navy Information Operations Command (NIOC) Norfolk, the Navy's Center of Excellence for IO, is responsible for providing operationally focused training; planning support and augmentation from the tactical to the strategic level; developing IO doctrine, tactics, techniques, and procedures; advocating requirements in support of future effects-based warfare; conducting experimentation for evaluating emerging or existing IO technologies and doctrine; providing and managing IO data for fleet operations. NIOC Norfolk operates under the operational and administrative control of NAVNETWARCOM, and has three subordinate commands: NIOC San Diego, NIOC Whidbey Island and Navy IO Detachment Groton.

- **Navy Cyber Defense Operations Command**

  The Navy Cyber Defense Operations Command (NCDOC), coordinates, monitors, and oversees the defense of Navy computer networks and systems, including telecommunications, and is responsible for accomplishing computer network defense (CND) missions as assigned by NAVNETWARCOM and Joint Task Force - Global Network Operations (JTF-GNO).

- **Navy Information Operations Command Suitland**

Navy Information Operations Command (NIOC) Suitland serves as Navy's IO innovation center and functions as the principal technical agent for research and development of prototype IO capabilities. NIOC Suitland supports the development capabilities encompassing all aspects of IO attack, protect, and exploit; maintaining an aggressive program to acquire and analyze state-of-the-art technologies (software and hardware), evaluate fleet applicability, and prototype developmental capabilities. NIOC Suitland maintains a collaborative relationship with Space and Naval Warfare Systems Command, Systems Center San Diego to provide efficient and effective technical expertise in command, control, communications, computers, and intelligence, surveillance, reconnaissance and information operations. NIOC Suitland also supports development coordination between NAVNETWARCOM, OPNAV, NIOC Norfolk, systems commands, IO technology center, and the commercial industry.

Last Updated: November 2009

Air Force Intelligence, Surveillance and Reconnaissance Agency

Air Force Intelligence, Surveillance and Reconnaissance Agency, with headquarters at Lackland Air Force Base, Texas, was activated June 8, 2007. Formerly known as Air Intelligence Agency, the new Air Force Intelligence, Surveillance and Reconnaissance Agency is aligned under the Headquarters United States Air Force/A2 (HQ USAF/A2) as a Field Operating Agency.

Mission

The agency's mission is to organize, train, equip, and present assigned forces and capabilities to conduct intelligence, surveillance and reconnaissance for combatant commanders and the nation. Implement and oversee execution of HQ USAF/A2 policy and guidance to expand Air Force ISR capabilities to meet current and future challenges.

Personnel

The agency's almost 17,000 people serve at approximately 72 locations worldwide.

Organization

The 70th Intelligence, Surveillance, and Reconnaissance Wing; 480th Intelligence, Surveillance and Reconnaissance Wing; 361st Intelligence, Surveillance and Reconnaissance Group; National Air and Space Intelligence Center (NASIC); and Air Force Technical Applications Center (AFTAC) are aligned under Air Force ISR Agency. The agency is also responsible for mission management and support of signals intelligence operations for the 67th Network Warfare Wing and the 688th Information Operations Wing, both subordinate to the 24th Air Force, and the 55th Wing, subordinate to the 8th Air Force. AF ISR Agency provides mission management and support for specific intelligence operations within these units. Mission support includes organizing, training and equipping the cryptologic elements of these organizations.

70th Intelligence, Surveillance, and Reconnaissance Wing
The 70th Intelligence Wing, with headquarters at Fort Meade, Md., integrates Air Force capabilities into global cryptologic operations, directly supporting national-level decision makers, combatant commanders and tactical warfighters. The wing works closely with the National Security Agency, leveraging the net-centric capabilities of a worldwide signals intelligence enterprise to conduct National-Tactical Integration for the joint and Air Force fight. The effect on the battlespace is immediate, high-impact and decisive. The wing includes seven operational intelligence groups located in the continental U.S., Pacific and European theaters. The wing was activated on Aug. 16, 2000.

National Air and Space Intelligence Center (NASIC)
The National Air and Space Intelligence Center, with headquarters at Wright-Patterson AFB, Oh., is the primary Department of Defense producer of foreign air and space intelligence. NASIC develops its products by analyzing all available data on foreign aerospace forces and weapons systems to determine performance characteristics, capabilities, vulnerabilities, and intentions. NASIC assessments are often an

important factor in shaping national security and defense policies. As the DoD experts on foreign aerospace system capabilities, the center also supports weapons treaty negotiations and verification. Since 1961 the center's mission and resources have expanded to meet the challenge of worldwide technological developments and the accompanying national need for aerospace intelligence. In recent years, the emphasis has increasingly shifted toward evaluation of worldwide aerospace systems and the production of tailored, customer-specific products.

480th Intelligence Wing
With headquarters at Langley AFB, Va., the 480th IW produces and provides timely, tailored intelligence data and capabilities to meet Air Force needs. As a dynamic, worldwide force multiplier, the wing delivers valuable information and analysis to U.S. combatants across the globe. The wing operates and maintains the AF Distributed Common Ground System (DCGS) also known as the "Sentinel" weapon system, and performs imagery intelligence, cryptologic and measurement and signatures intelligence activities, targeting and general intelligence production, intelligence data handling system network operations, and data/product dissemination. Subordinate to the wing are five intelligence groups located in the continental U.S, Pacific, and European theaters. The wing was activated Dec. 1, 2003.

361st Intelligence, Surveillance, and Reconnaissance Group
With headquarters at Hurlburt Field, Fl., the vision of the 361st ISRG is to be the Special Operations Force's community premier provider of specialized ISR capabilities. They train, equip, and present over 250 Airmen to provide specialized SOF ISR forces for worldwide employment.

Air Force Technical Applications Center (AFTAC)
The Air Force Technical Applications Center, with headquarters at Patrick AFB, Fla., performs nuclear treaty monitoring and nuclear event detection. AFTAC provides national authorities quality technical measurements to monitor nuclear treaty compliance and develops advanced proliferation monitoring technologies to preserve our nation's security. AFTAC has been performing its nuclear event detection mission since its inception in 1973.

688th Information Operations Wing
With headquarters at Lackland AFB, Texas, the 688th IOW, formerly known as the Air Force Information Operations Center, was activated on Aug. 18, 2009 and is engaged in myriad activities as the Air Force's information operations executive agent, including integrating information operations tactics, training and technology for combatant commanders. The center is comprised of approximately 1,000 military and civilian members trained in the areas of operations, engineering, operations research, intelligence, radar technology, and communications and computer applications.

67th Network Warfare Wing
With headquarters also at Lackland AFB, the 67th IW has a global mission. As the USAF's cyberspace force, the 67th NWW's mission is to organize, train, and equip cyberspace forces to conduct network defense, attack, and exploitation. It also executes full-spectrum Air Force network operations, training, tactics, and management for AFNetOps/CC and combatants CCs. While the 67th NWW is subordinate to the 24th AF, the AF ISR Agency/CC, as the AF Service Cryptologic Component, maintains cryptologic authority over the 67th NWW's Signals Intelligence mission.

55th Wing
With headquarters at Offutt AFB, Neb., the 55th Wing's mission is to provide dominant intelligence, surveillance, and reconnaissance; electronic attack; command and control; and precision awareness to national leadership and warfighters across that spectrum of conflict any time, any place. The 55th Wing also provides Presidential support and international treaty verification as directed by the President, Secretary of Defense, Joint Chiefs of Staff, theater combatant commanders, commanders of major Air Force commands and national intelligence agencies. While the 55th Wing is subordinate to the 8th AF, the

AF ISR Agency/CC, as the AF Service Cryptologic Component, maintains cryptologic authority over the wing's Signals Intelligence mission.

Point of Contact
Air Force ISR Agency, Public Affairs Office; 102 Hall Blvd, Ste 272; San Antonio, TX 78243-7089; DSN 969-2166 or (210) 977-2166.

Last updated: October 2009

This Page Intentionally Blank

Headquarters 24th Air Force

The 24th Air Force (24 AF) is the operational warfighting organization responsible for conducting the full range of cyber operations. 24 AF establishes, operates, maintains and defends the Air Force provisioned portion of the DoD network to ensure the Joint Warfighter can maintain the information advantage while prosecuting military operations. The 24 AF mission is: Assure Joint Warfighter freedom of action, establish, extend, operate and defend assigned portion of the DoD network, and provide capabilities in, through, and from cyberspace.

On October 6, 2008, following its annual Corona conference, the Air Force announced, a numbered air force, 24 AF, would gain the cyber warfare mission as part of Air Force Space Command (AFSPC). The 24 AF is the newest numbered air force; it celebrated its standup on 18 August 2009. This is the Air Force's first-ever unit designated for the sole purpose of cyberspace operations.

The 24 AF is located at Lackland AFB, TX and has three subordinate wings, the 67th Network Warfare Wing (67 NWW), located at Lackland AFB, TX, the 688th Information Operations Wing (688 IOW), also located at Lackland AFB, TX, and the 689th Combat Communications Wing (689 CCW) at Robins AFB, Georgia. The 24 AF oversees 5,400 Airmen to conduct or support 24-hour operations involving cyberspace operations, including 3,339 military, 2,975 civilian and 1,364 contractor personnel. In addition, more than 10,000 Air National Guard and Air Force Reserve personnel directly support the 24 AF and AFSPC mission.

The 624th Operations Center (624 OC), collocated with the 24 AF at Lackland AFB, TX serves as the 24 AF's operational arm to provide a robust full-spectrum and integrated cyberspace operations capability. The 624 OC interfaces with theater and functional Air Operations Centers to establish, plan, direct, coordinate, assess, and command & control cyber operations in support of AF and Joint warfighting requirements.

The 67 NWW is charged as the Air Force execution element for Air Force Network Operations and providing network warfare capabilities to Air Force, Joint Task Force and combatant commanders that operate, manage, and defend global Air Force networks. Additionally, the 67 NWW performs electronic systems security assessments for the Air Force and Joint community. As the Air Force's only network warfare wing, it has Airmen around the world conducting and supporting cyber operations. The wing is composed of three groups, 12 squadrons, one flight, and several detachments with more than 2,000 Airmen executing the Cyber portion of the Air Force mission.

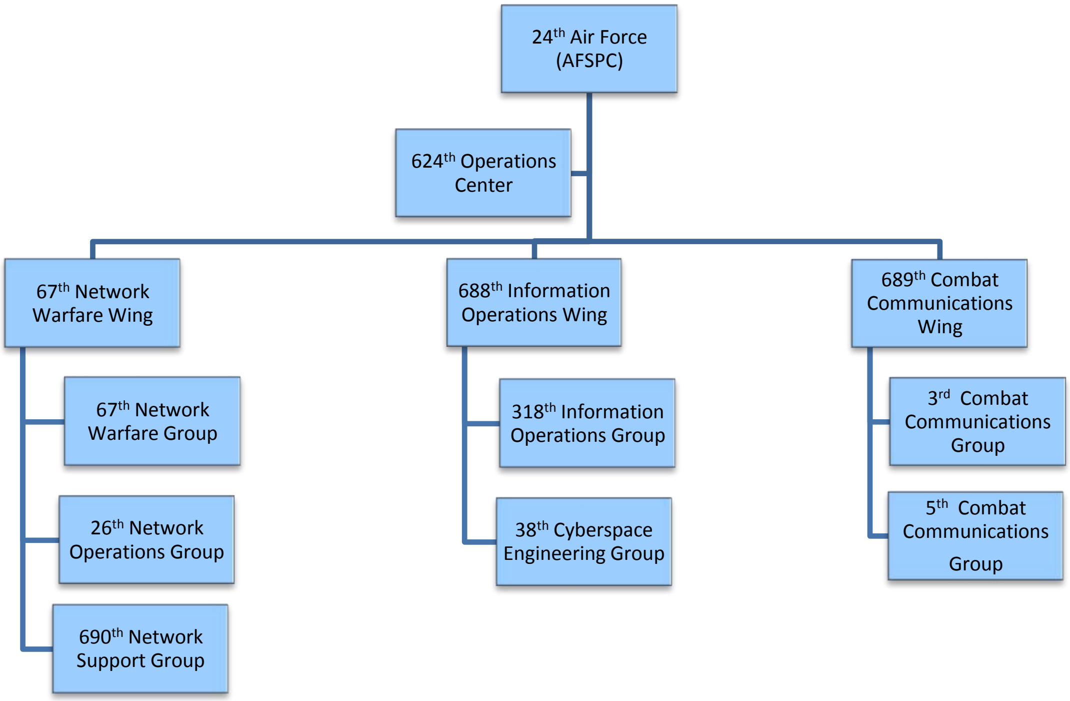
The 688 IOW is comprised of two groups: the 318th Information Operations Group (318 IOG) and the 38th Cyberspace Engineering Group (38 CEG). The 318 IOG is the Air Force's center of excellence for information operations. They are responsible for creating the information operations advantage for combatant forces through exploring, developing, applying and transitioning counter information technology, strategy, tactics and data to control the information battlespace and provide the world's best IO leaders. The 38 CEG is the Air Force's premier Engineering Installation Group providing engineering solutions to customers world-wide at every level of command.

The 689th Combat Communications Wing, headquartered at Robins Air Force Base, Georgia delivers combat communications for the joint and coalition warfighter supporting combat operations and Humanitarian Relief Operations. The wing has a total-service wartime capability that encompasses more than $600 million dollars worth of materiel and 50 Air Force units comprised 6,000 Airmen who provide combat communications and Air Traffic Control and Landing Systems capabilities in the Continental United States and Abroad

Point of Contact:

24th Air Force Public Affairs, 467 Moore Street, Bldg. 2167, Lackland AFB, Texas, CML 210-395-7020, DSN 969-7020.

ORGANIZATION:


24th Air Force (AFSPC)
624th Operations Center
67th Network Warfare Wing
688th Information Operations Wing
689th Combat Communications Wing
67th Network Warfare Group
26th Network Operations Group
690th Network Support Group
318th Information Operations Group
38th Cyberspace Engineering Group
3rd Combat Communications Group
5th Combat Communications Group

Last Updated: October 2009

67th Network Warfare Wing

The 67th Network Warfare Wing (67 NWW), headquartered at Kelly Field Annex, Lackland AFB, San Antonio, Texas, executes a new mission that includes the integrated planning and employment of military capabilities to achieve the desired effects across the interconnected analog and digital portion of the Battlespace—Air Force Network Ops. The Wing's Cyber Warriors conduct network operations through the dynamic combination of hardware, software, data, and human interaction that involves time-critical, operational-level decisions that direct configuration changes and information routing.

The 67 NWW, headquartered at Kelly Field Annex, Lackland AFB, TX, is the Air Force's only Network Warfare Wing. The wing employs 2,500 military and civilian Air Force Space Command personnel in 25 locations worldwide. As the 24 AF's execution arm for AF Net Ops, the wing readies and employs Airmen to conduct network defense and full spectrum network ops and systems telecommunications monitoring for AF and combatant commanders.

The wing consists of the 67th Network Warfare Group, 26th Network Operations Group, and 690th Network Support Group. Activated in 1947, the wing conducted Tactical Reconnaissance and later was the only wing of its type in Korea during the Korean War. The wing later trained Air Force and other countries aircrews in the RF-4C Phantom. One squadron of the wing saw combat action during Operations DESERT SHIELD and DESERT STORM. In 1993, the Wing was redesignated as the 67th Intelligence Wing and was the largest wing in the Air Force at the time. In 2000, the wing was assigned the mission of Information Operations becoming the Air Force's first IO Wing. In July 2006, the wing became the Air Force's first and only Network Warfare Wing executing the Cyber portion of the Air Force mission to Fly, Fight, and Win in Air, Space and Cyberspace.

Last Updated: October 2009

This Page Intentionally Blank

688th Information Operations Wing

The 688th Information Operations Wing (688 IOW) is located at Lackland AFB, San Antonio, Texas. The wing's mission statement is: Deliver proven Information Operations and Engineering Infrastructure capabilities integrated across air, space and cyberspace domains. The wing was formally designated on 18 August 2009. The 688 IOW was originally activated as the 6901st Special Communication Center in July 1953, and became the Air Force Electronic Warfare Center in 1975. Air Force successes in exploiting enemy information systems during Operation Desert Storm led to the realization that the strategies and tactics of command and control warfare could be expanded to the entire information spectrum and be implemented as information warfare. In response, the Air Force Information Warfare Center (AFIWC) was activated on 10 September 1993, combining technical skill sets from the former Air Force Electronic Warfare Center (AFEWC) with the Air Force Cryptologic Support Center's Securities Directorate and intelligence capabilities from the former Air Force Intelligence Command. On 1 October 2006, AFIWC, was re-designated the Air Force Information Operations Center (AFIOC). The name was changed to better reflect the center's continued advancements in network warfare, electronic warfare and influence operations missions. AFIOC was re-designated as the 688 IOW on 18 August 2009 and aligned under 24th Air Force.

The wing is composed of two groups: the 318th Information Operations Group (IOG) at Lackland AFB and the 38th Cyberspace Engineering Group (CEG) at Tinker AFB. The 318 IOG explores new cyberspace technologies to engineer next-generation weapons capabilities for operational warfighters. It has a test squadron for developmental and operational test and evaluation, a tactics squadron to optimize IO tactics, techniques, and procedures for weapon systems, a school house to arm the next generation of cyber warriors with the most up to date information, and an assessment squadron to identify and mitigate vulnerabilities on AF systems.

The 38 CEG is the Air Force's premier Engineering and Installation group provides systems telecommunications managers to every Combatant Command, Major Command, and Air Force base worldwide. Their Special Engineering Branch provides unique communications solutions to a variety of customers worldwide. The group was formerly the 38th Engineering Installation Group under Air Force Materiel Command. Newly added to the 38 CEG, the 85th Engineering Installation Squadron at Keesler AFB, MS, is a team of nearly 100 military members who are tasked to deploy engineering solutions anywhere in the world within 72 hours.

The wing's team of more than 1200 military and civilian members is skilled in the areas of engineering installation, weaponeering, operations research, intelligence, communications and computer applications.

Last Updated: October 2009

This Page Intentionally Blank

689th Combat Communications Wing

The 689th Combat Communications Wing (689 CCW) is located at Robins Air Force Base, Warner Robins, Georgia. The 689 CCW's mission statement: Deliver combat communications for the joint/coalition war fighter supporting combat operations and Humanitarian Relief Operations…anytime…anywhere!

The unit traces it linage to the 1931st Airways and Air Communications Squadron which was originally designated in 1948. It was later re-designated as the 1931st Communications Squadron in 1961. Then, in 1969, the squadron grew and was again re-designated as the 1931st communications Group. The 1931st would go through several more re-designations due to the demands of the Air Force before finally being de-activated on 26 September 1991. During its lifespan, the 1931st served with distinction in the Alaskan Communications region, Air Force Communications Command, 21st Fighter Wing. The distinguished service of the 1931st was recognized with the award of the Air Force Outstanding Unit Award eight times. The wing resumed its history and was reactivated and redesignated on 5 October, 2009 as the 689 CCW under 24th Air Force and Air Force Space Command.

The 689 CCW has brought together, as one cohesive team, several active and reserve subordinate units with their own storied histories and over 150 major awards. Active Duty units include the 3rd Combat Communications Group and the 5th Combat Communications Group. Air National Guard partners consist of the 162nd, 201st, 226th, 251st , 252nd, 253rd, 254th, and 281st Combat Communications Groups and the 224th and 290th Joint Communications Support Squadrons. Air Force Reserve units include 23rd Combat Communications Squadron, 35th Combat Communications Squadron, 42nd Combat Communications Squadron, and 55th Combat Communications Squadron.

The Wing current has a war time projection force of more than 6,000 skilled Airmen (1,500 AD & 4,500 ARC), armed with over $600 million dollars worth of materiel, who provide tactical communications, computer systems, navigational aids, and Air Traffic Control (ATC) services anywhere in the world to meet of the Air Force, Department of Defense, and other US Commitments. Total Force Team members, including DoD civilians and contractors are trained to deploy more than 150 mission systems providing initial services to deployed customers at various units under hostile conditions in austere locations where communications and ATC capabilities are not established.

Last Updated: October 2009

This Page Intentionally Blank

Information Operations Conditions (INFOCONs)

Preface. CDRUSSTRATCOM has directed the replacement of Strategic Directive (SD) 527-1, "Department of Defense (DoD) Information Operations Condition (INFOCON)" with Strategic Instruction (SI) 720-3, "DoD Cyber Condition (CYBERCON)". SI 720-3 is currently under development by USSTRATCOM and is expected to publish in August 2010. SD 527-1 will remain in effect until superseded by SI 720-3 or otherwise cancelled by CDRUSSTRATCOM.

The major difference between INFOCON and CYBERCON is that where INFOCON measures and actions are more defensive (CND) in nature, the measures and actions of CYBERCON will use the full spectrum of information operations to include CND, computer network exploitation (CNE), operational preparation of the environment (OPE), CND Response Actions (RA) and CNA as authorized by DoD regulations.

1. Introduction. The INFOCON system is a commander's alert system that establishes a uniform process for posturing and defending against malicious activity targeted against U.S. DoD information systems and networks. The INFOCON system was developed for U.S. DoD information systems and networks. However, it is acknowledged that U.S. involvement in future conflicts will likely be within a Combined operations environment. This implies that the success of the Warfighting operations will depend greatly on the ability of the U.S. and allied/coalition partners to ensure continued availability and access to critical mission and support information systems and information networks.

2. Description. The INFOCON system is a commander's alert system, characterized by five progressive levels of threats to information networks, and a series of increasing defensive measures that apply to information systems and, to a lesser extent, users of these systems. Specific features assist the commander in using the INFOCON system. A risk mitigation tool aids the commander in proactively declaring postures and directing defensive actions based on advanced indications and warning of hostile activity. The INFOCON system also guides the commander in identifying the INFOCON posture in the event predictive intelligence is not possible. The uniform application of defensive measures promotes predictable responses to crises and provides timely, accurate, and clear direction to commanders. Flexibility is built into the INFOCON system to allow additional specific actions to be mandated, based on the threat. Thus, the INFOCON system provides a range of defensive measures that support operations at all levels of conflict, peacetime operations through combat operations, and back to restoration of peace. The INFOCON system pertains to all information systems and networks, including interconnections between public and coalition networks.

3. Strategy. The INFOCON strategy is a "readiness-based," proactive approach. This paradigm shift represents a significant change in how commanders at all levels ensure the security and operational readiness of their information networks. CDRUSSTRATCOM directs changes in the global INFOCON status, while changes in local or regional INFOCON status will be more actively managed by commanders at all levels (e.g., base, post, camp, station, major command) using a framework of standardized measures. INFOCON 5 is normal readiness and INFOCON 1 is maximum readiness. Each level represents an increasing level of network readiness based on tradeoffs in resource balancing that every commander must make. The INFOCON are supplemented by Tailored Readiness Options (TROs), which are applied in order to respond to specific intrusion characteristics or activities, directed by CDRUSSTRATCOM or commanders.

The INFOCON system is predicated on the fact that a determined intruder will always compromise a networked system. Returning the system to a pristine, baseline state restores confidence in the system. Any system changes, while not always easily detectable in isolation, are almost always detectable by comparing the current status to a previous known baseline. However, maintaining a baseline snapshot across an enterprise and running the appropriate comparisons are non-trivial tasks for network and system administrators. As such, the readiness posture becomes a resource balance of how often commanders want to ensure their networks (or portions thereof) are free of malicious activity in relation to their own Operational Tempo (OPTEMPO). The readiness postures are designed to provide commanders at all levels the flexibility to set the readiness level they deem most appropriate for their OPTEMPO and available resources.

4. Posture Levels.

a. INFOCON 5. INFOCON 5 is characterized by routine NetOps normal readiness of information systems and networks that can be sustained indefinitely. Information networks are fully operational in a known baseline condition with standard information assurance policies in place and enforced.

b. INFOCON 4. INFOCON 4 increases NetOps readiness, in preparation for operations or exercises, with a limited impact to the end user. System and network administrators will establish an operational rhythm to validate the known good image of an information network against the current state and identify unauthorized changes. By increasing the frequency of this validation process, the state of an information network is confirmed as unaltered (i.e., good) or determined to be compromised.

c. INFOCON 3. INFOCON 3 further increases NetOps readiness by increasing the frequency of validation of the information network and its corresponding configuration. Impact to end-users is minor.

d. INFOCON 2. INFOCON 2 is a readiness condition requiring a further increase in frequency of validation of the information network and its corresponding configuration. The impact on system administrators will increase in comparison to INFOCON 3 and will require an increase in preplanning, personnel training, and the exercising and pre-positioning of system rebuilding utilities. Impact to end-users could be significant for short periods, which can be mitigated through training and scheduling.

e. INFOCON 1. INFOCON 1 is the highest readiness condition and addresses intrusion techniques that cannot be identified or defeated at lower readiness levels (e.g., kernel root kit). It should be implemented only in those limited cases where INFOCON 2 measures repeatedly indicate anomalous activities that cannot be explained except by the presence of these intrusion techniques. Currently, the most effective method for ensuring the system has not been compromised in this manner is to reload operating system software on key infrastructure servers (e.g., domain controllers, Exchange servers, etc.) from an accurate baseline.

5. Authority. The INFOCON system is established by the Secretary of Defense (SecDef), and administered by the Commander, United States Strategic Command (CDRUSSTRATCOM). The INFOCON system will be administered through the Commander, Joint Task Force - Global Network Operations (JTF-GNO). All combatant commands, services, directors of Defense and combat support agencies will develop supplemental INFOCON procedures as required, specific to their command and in consonance with Strategic Command Directive (SD) 527-1, *DEPARTMENT OF DEFENSE (DoD) INFORMATION OPERATIONS CONDITION (INFOCON) SYSTEM PROCEDURES (U/FOUO).* SD 527-1 can be found on the JTF-GNO SIPRNet webpage:

http://www.jtfgno.smil.mil/site/index.cfm?Page=INFOCON

Subordinate and operational unit commanders will use the INFOCON procedures developed by their higher headquarters (e.g., combatant commands or Services). Existing policy and procedures on communications security (COMSEC) may be integrated into local INFOCON procedures at the commander’s discretion.

6. Applicability. The established INFOCON procedures (SD 527-1) applies to the Office of the Secretary of Defense, the Services, the Joint Staff, the Combatant Commands, the Defense Agencies, the DoD Field Activities, and all other organizational entities (hereafter referred to collectively as "the Components) who are connected to the DoD Global Information Grid (GIG).

7. Structure. This paragraph explains the INFOCON structure, including level and recommended actions.

a. INFOCON 5, NORMAL READINESS.

INFOCON 5

5-1: Re-establish 'secure baseline' in conjunction with a check for unauthorized changes on a semi-annual (180-day) cycle. This should involve mirroring the drives for subsequent examination, prior to re-loading the secure configuration. If examination of the drives indicates unauthorized changes, first determine if the changes were actually authorized, yet improperly recorded. Unauthorized changes may indicate the need to temporarily increase to a higher INFOCON level, depending on what unauthorized changes are discovered.

5-2. Ensure all Information Systems are compliant with guidance and responsibilities outlined within IAW I O-8530.2, *Support to Computer Network Defense* and CJCS Manual 6510.01, *Defense-in-Depth: Information Assurance (IA) and Computer Network Defense (CND).*

5-3. When moving into/from a higher INFOCON level, acknowledge receipt, report entry into INFOCON Level activities via operational channels to the declaring command.

5-4. Through automated and procedural means, update and maintain a current database of critical network infrastructure equipment used to maintain the network and a representative sampling of workstations

5-5. Perform operational impact assessment on all mission critical, mission support, and administrative information systems and networks.

5-6. Conduct routine vulnerability assessments.

b. INFOCON 4, INCREASED MILITARY VIGILANCE.

INFOCON 4

4-1. Acknowledge receipt/entry into INFOCON 4 and report completion of the first INFOCON 4 cycle.

4-2. Confirm completion of directive measures at previous INFOCON levels.

4-3. Establish exit criteria. (Declaring Command)

4-4. Implement TROs as specified in the implementing message or by regional/local commanders.

4-5. On a 90 day cycle: Upon notification immediately complete the following activities and then every 90 days thereafter. Using manual methods or available automated tools, identify and verify all changes to the system parameters tracked using the database created at INFOCON 5.-4

4-6. If explicit permissions are used on folders or files also check to ensure permissions have not been modified.

c. INFOCON 3, ENHANCED READINESS.

INFOCON 3

3-1. Acknowledge receipt and entry into INFOCON 3 and report completion of the first INFOCON 3 cycle

3-2. Confirm completion of directive measures at previous INFOCON levels to the declaring Command.

3-3. Establish exit criteria for current INFOCON level (Declaring Command)

3-4. Implement TROs as specified by implementing message or regional/local commanders.

3-5. Re-establish a secure baseline on a 60-day cycle.

d. INFOCON 2, GREATER READINESS.

INFOCON 2

2-1. Acknowledge receipt and entry into INFOCON 2 and report completion of the first INFOCON 2 cycle.

2-2. Confirm completion of directive measures at previous INFOCON levels to the declaring Command.

2-3. Establish exit criteria for current INFOCON level. (Declaring Command)

2-4. Implement TROs as specified by implementing message or regional/local commanders.

2-5. Re-establish a secure baseline on a 30-day cycle.

e. INFOCON 1, MAXIMUM READINESS.

INFOCON 1

1-1. Acknowledge receipt and entry into INFOCON 1 and report completion of the first INFOCON 1 cycle.

1-2. Confirm completion of directive measures at previous INFOCON levels to the declaring Command.

1-3. Establish exit criteria for current INFOCON level. (Declaring Command)

1-4. Implement TROs as specified by implementing message or regional/local commanders.

1-5. Re-establish a secure baseline on a 15-day cycle.

8. Procedures.

a. Determining the INFOCON. The foremost determining criteria for changing an INFOCON level is the anticipated operational activity and the degree to which those activities are reliant on networked resources. INFOCON levels should be raised prior to the activity to ensure the network is as ready as possible when the operation or exercise begins. Because system and network administrators implement many of the INFOCON measures over a period of time in a pre-determined operational rhythm, commanders should raise INFOCON levels early enough to ensure completion of at least one cycle before the operational activity begins. Recommendations for possible INFOCON changes should be written into OPLANs and CONPLANs.

(1) Commanders should consider OPSEC when determining INFOCON levels to ensure OPSEC and INFOCON processes are coordinated to protect operations. Regional and local commanders should consider whether INFOCON changes provide an indicator(s) to an adversary and increase INFOCON levels on a random basis to ensure the establishment of INFOCON levels does not become an indicator of planned activity.

(2) Regional or local commanders who are operating in support of other commands shall consider raising the INFOCON levels of all or key portions of their assets to match the level of the supported commander.

(3) The INFOCON system focuses on readiness but threats to the network should still be a consideration for changing INFOCON levels. Indications and Warning or the detection of new network activity from open sources or network sensors represent threats to network readiness.

b. Declaring INFOCONs. The Commander, Joint Task Force - Global Network Operations (CDR JTF-GNO) will recommend changes in INFOCON to CDRUSSTRATCOM. Prior to this recommendation, JTF-GNO will coordinate with the Components to determine the operational impact of changing the INFOCON level. Upon receiving the recommendation from CDR JTF-GNO, CDRUSSTRATCOM will assess, and if necessary, direct a -level INFOCON change. USSTRATCOM will notify Components of a level INFOCON change via a CNEC and/or an INFOCON Alert message. Regional combatant commanders who independently raise INFOCON levels will notify USSTRATCOM (cc JTF-GNO), other combatant commanders, and the services to provide situational awareness and allow them to consider matching the regional level to better support operations.

c. Response Measures.

(1) Common Directive Measures. Actions common to all Components have been identified for each INFOCON level. The directive measures provide a common readiness posture across information systems and networks.

(2) Order of Implementation. When a non-sequential increase in INFOCONs occurs (e.g. from 5 to 3), the directive measures from the skipped INFOCON level(s) will be accomplished. Once the higher INFOCON level has been achieved the lower (skipped) INFOCON level will complete by default.

(3) Directive Measure Exemptions. Components will normally accomplish all actions for the INFOCON level declared. However, local operational realities may require that a commander delay, or even omit implementation of specific INFOCON directive measures. The commander declaring the INFOCON will be informed by subordinate commands of any deviations and/or exemptions from directive measures or any additional actions directed by CDRUSSTRATCOM in the INFOCON Change Alert Message.

(4) Tailored Readiness Options (TROs). In addition to the directive measures the declaring commander may direct the implementation of TROs to counter a specific threat, by region or globally. TROs are supplemental measures to respond to specific intrusion characteristics directed either by CDRUSSTRATCOM or the responsible regional/local commander. They are narrowly focused and meant to supplement the current INFOCON readiness level either globally, regionally or at bases/camps/posts/ stations. Normally, TROs supplement a lower INFOCON level.

(5) Pre-coordination of Directive Measures. To expedite INFOCON change actions, all supporting combatant command, service and/or agency units will establish a Memorandum of Agreement or directive to pre-coordinate INFOCON procedures and directive measures with the unified

commander(s) they support. The coordination should include a determination of which actions may be implemented immediately, and which actions require combatant commander notification prior to implementation. This same process applies to all activities under Host/Tenant agreements, as well as organizations employing cross-domain solutions to connect between different security domains or other trust relationships.

d. Reporting. Technical reporting will be accomplished IAW SD 527-1, Chapter 5, Sample Reporting Templates. INFOCONs assess potential and/or actual impact to operations and must be reported through operational channels. Additional guidance on INFOCON reporting follows.

(1) Reporting Channels. Combatant commands, Services, and agencies will report INFOCON changes and SITREPs to the CDR, USSTRATCOM: USSTRATCOM OFFUTT AFB NE//CC//.

(2) Reporting Frequency. Services, combatant commands, and Defense agencies will report acknowledgement of INFOCON change alert upon receipt of INFOCON Alert Message using the INFOCON Change Acknowledgement SITREP. Services, combatant commands, and Defense agencies will report INFOCON status changes using the INFOCON Status SITREP.

(3) Report Formats. Examples of report formats can be found in SD 527-1, Chapter5, Sample Reporting Templates.

(4) Dissemination of INFOCON. USSTRATCOM will notify Components of a -level INFOCON change via a CNEC and/or an INFOCON Alert message. Commands, Services, and agencies are responsible for notifying units assigned to them.

9. Security. Classification guidance and disclosure policy concerning IO is addressed in DoDI 3600.2, *Classification Guidance for Information Operations*. Specific guidance related to INFOCON follows.

a. INFOCON labels and descriptions are unclassified.

b. Generic defensive measures, when not tied to a specific INFOCON, are unclassified. Specific measures may be published in a classified appendix, if required.

c. Measures to be taken by all personnel, regardless of INFOCON, are unclassified.

d. General criteria to declare an INFOCON are FOR OFFICIAL USE ONLY (FOUO). Specific criteria may be published in a classified appendix, if required.

e. Classification of the measures associated with a particular INFOCON is the responsibility of the originator and will be classified according to content. However, the measures associated with a particular INFOCON, in aggregate, may require a higher classification than the individual measures. The measures associated with a particular INFOCON, in aggregate, will be FOUO at a minimum.

f. The operational impact of a successful information attack is classified SECRET or higher.

g. CNA intelligence assessments are classified SECRET or higher.

h. Information associated with an ongoing criminal investigation of a CNA may be considered law-enforcement sensitive.

i. A combatant command, service, or agency may authorize release of its INFOCON system and procedures to allies or coalition partners as necessary to ensure effective protection of its information systems. Locally developed INFOCON procedures should use DoDI 3600.2 and the guidance above when considering release to allies or coalition partners.

j. Changes in INFOCON are operational security (OPSEC) indicators and must be protected accordingly. The criteria and response measures are also of value to foreign intelligence Services in assessing the effectiveness of a CNA and in analyzing response. Do not post INFOCON procedures in publicly accessible locations such as unit web pages on unclassified networks and bulletin boards accessible to outsiders.

10. Relationship of INFOCON to Other Alert Systems. The INFOCON, THREATCON, DEFCON, CNA-WATCHCON, and conventional WATCHCON all interact with each other when the situation warrants it. The INFOCON may be changed based on the world situation (THREATCON, DEFCON), the intelligence community's level of concern (CNA-WATCHCON, conventional WATCHCON), or other factors. Likewise, a change in INFOCON may prompt a corresponding change in other alert systems.

a. The defense condition (DEFCON) is a uniform system of progressive conditions describing the types of actions required to bring a command's readiness to the level required by the situation.

b. The threat condition (THREATCON) is a process that sets the level for a terrorist threat condition at a given location, based on existing intelligence and other information.

c. A watch condition (WATCHCON) is part of the defense warning system indicating the degree of intelligence concern with a particular warning problem.

d. A CNA-WATCHCON is an intelligence assessment that takes into account CNA threat levels, as well as the overall political situation (reference CJCSM 3402.01A, "Alert System of the Chairman of the Joint Chiefs of Staff").

e. The INFOCON addresses risk of attack and protective measures for information and information systems.

Last Updated: October 2009

This Page Intentionally Blank

Glossary

Area of influence

A geographical area wherein a commander is directly capable of influencing operations by maneuver or fire support systems normally under the commander’s command or control. (JP 1-02)

Area of interest

That area of concern to the commander, including the area of influence, areas adjacent thereto, and extending into enemy territory to the objectives of current or planned operations. This area also includes areas occupied by enemy forces who could jeopardize the accomplishment of the mission. Also called AOI. See also area of influence. (JP 1-02)

Civil affairs (CA)

Designated Active and Reserve component forces and units organized, trained, and equipped specifically to conduct civil affairs activities and to support civil-military operations. Also called **CA**. (JP 1-02)

Civil military operations (CMO)

The activities of a commander that establish, maintain, influence, or exploit relations between military forces, governmental and nongovernmental civilian organizations and authorities, and the civilian populace in a friendly, neutral, or hostile operational area in order to facilitate military operations, to consolidate and achieve operational US objectives. Civil-military operations may include performance by military forces of activities and functions normally the responsibility of the local, regional, or national government. These activities may occur prior to, during, or subsequent to other military actions. They may also occur, if directed, in the absence of other military operations. Civil-military operations may be performed by designated civil affairs, by other military forces, or by a combination of civil affairs and other forces. Also called **CMO.** (JP 1-02)

Combat Camera (COMCAM)

The acquisition and utilization of still and motion imagery in support of combat, information, humanitarian, special force, intelligence, reconnaissance, engineering, legal, public affairs, and other operations involving the Military Services. Also called COMCAM. (JP 3-13)

Command and control (C2)

The exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission. Command and control functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission. (JP1- 02)

Command and control system (C2)

The facilities, equipment, communications, procedures, and personnel essential for planning, directing, and controlling operations of assigned forces pursuant to the missions assigned. (JP 1-02)

Computer network attack (CNA)

Actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves. Also called **CNA.** (JP 1-02)

Computer network defense (CND)

Actions taken through the use of computer networks to protect, monitor, analyze, detect and respond to unauthorized activity within Department of Defense information systems and computer networks. Also called **CND.** See also **computer network attack; computer network exploitation; computer network operations.** (JP 1-02)

Computer network exploitation (CNE)

Enabling operations and intelligence collection to gather data from target or adversary automated information systems or networks. (JP 1-02)

Computer network operations (CNO)

Comprised of computer network attack, computer network defense, and related computer network exploitation enabling operations. (JP 1-02)

Computer security (COMPUSEC)

The protection resulting from all measures to deny unauthorized access and exploitation of friendly computer systems. (JP 1-02)

Counterdeception

Efforts to negate, neutralize, diminish the effects of, or gain advantage from a foreign deception operation. Counterdeception does not include the intelligence function of identifying foreign deception operations. (JP 1-02)

Counterintelligence

The information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassination conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities. (JP 1-02)

Counterpropaganda operations

Those psychological operations activities that identify adversary propaganda, contribute to situational awareness, and serve to expose adversary attempts to influence friendly populations and military forces. (JP 1-02)

Cyber counterintelligence

Measures to identify, penetrate, or neutralize foreign operations that use cyber means as the primary tradecraft methodology, as well as foreign intelligences service collection efforts that use traditional methods to gauge cyber capabilities and intentions. (JP1-02)

Cyberspace

A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. (CJCS CM-0363-08) (JP 1-02)

Cyberspace operations

The employment of cyber capabilities where the primary purpose is to achieve military objectives or effects in or through cyberspace. Such operations include computer network operations and activities to operate and defend the Global Information Grid.

Deception action

A collection of related deception events that form a major component of a deception operation. (JP 1-02)

Deception concept

The deception course of action forwarded to the Chairman of the Joint Chiefs of Staff for review as part of the combatant commander's strategic concept. (JP 1-02)

Deception course of action

A deception scheme developed during the estimate process in sufficient detail to permit decision-making. At a minimum, a deception course of action will identify the deception objective, the deception target, the desired perception, the deception story, and tentative deception means. (JP 1-02)

Deception event

A deception means executed at a specific time and location in support of a deception operation. (JP 1-02)

Deception means

Methods, resources, and techniques that can be used to convey information to the deception target. There are three categories of deception means: a. physical means Activities and resources used to convey or deny selected information to a foreign power. b. technical means Military materiel resources and their associated operating techniques used to convey or deny selected information to a foreign power. c. administrative means Resources, methods, and techniques to convey or deny oral, pictorial, documentary, or other physical evidence to a foreign power. (JP 1-02)

Deception objective

The desired result of a deception operation expressed in terms of what the adversary is to do or not to do at the critical time and/or location. (JP 1-02)

Deception story

A scenario that outlines the friendly actions that will be portrayed to cause the deception target to adopt the desired perception. (JP 1-02)

Deception target

The adversary decision maker with the authority to make the decision that will achieve the deception objective. (JP 1-02)

Defense support to public diplomacy (DSPD)

Those activities and measures taken by the Department of Defense components to support and facilitate public diplomacy efforts of the United States Government. (JP 1-02)

Desired Effects

The damage or casualties to the enemy or materiel that a commander desires to achieve from a nuclear weapon detonation. Damage effects on materiel are classified as light, moderate, or severe. Casualty effects on personnel may be immediate, prompt, or delayed.

Desired perceptions

In military deception, what the deception target must believe for it to make the decision that will achieve the deception objectives. (JP 1-02)

Disinformation

(Army) Disinformation is information disseminated primarily by intelligence organizations or other covert agencies designed to distort information, or deceive or influence US decision makers, US forces, coalition allies, key actors or individuals via indirect or unconventional means. (FM 3-13)

DoDD

Department of Defense Directive.

Electromagnetic pulse (EMP)

The electromagnetic radiation from a strong electronic pulse, most commonly caused by a nuclear explosion that may couple with electrical or electronic systems to produce damaging current and voltage surges. (JP 1-02)

Electromagnetic spectrum

The range of frequencies of electromagnetic radiation from zero to infinity. It is divided into 26 alphabetically designated bands. (JP 1-02)

Electronics security

The protection resulting from all measures designed to deny unauthorized persons information of value that might be derived from their interception and study of non communications electromagnetic radiation, e.g., radar (JP 1-02)

Electronic warfare (EW)

Any military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. Also called **EW.** The three major subdivisions within electronic warfare are: electronic attack, electronic protection, and electronic warfare support. a. **electronic attack.** That division of electronic warfare involving the use of electromagnetic energy, directed energy, or antiradiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability and is considered a form of fires. Also called **EA.** EA includes: 1) actions taken to prevent or reduce an enemy's effective use of the electromagnetic spectrum, such as jamming and electromagnetic deception, and 2) employment of weapons that use either electromagnetic or directed energy as their primary destructive mechanism (lasers, radio frequency weapons, particle beams). b. **electronic protection.** That division of electronic warfare involving passive and active means taken to protect personnel, facilities, and equipment from any effects of friendly or enemy employment of electronic warfare that degrade, neutralize, or destroy friendly combat capability. Also called **EP.** c. **electronic warfare support.** That division of electronic warfare involving actions tasked by, or under direct control of, an operational commander to search for, intercept, identify, and locate or localize sources of intentional and unintentional radiated electromagnetic energy for the purpose of immediate threat recognition, targeting, planning and conduct of future operations. Thus, electronic warfare support provides information required for decisions involving electronic warfare operations and other tactical actions such as threat avoidance, targeting, and homing. Also called **ES.** Electronic warfare support data can be used to produce signals intelligence, provide targeting for electronic or destructive attack, and produce measurement and signature intelligence. (JP 1-02)

Global information grid (GIG)

The globally interconnected, end-to-end set of information capabilities, associated processes and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel. The Global Information Grid includes owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services and National Security Systems. (JP 1-02)

Global information infrastructure

The worldwide interconnection of communications networks, computers, databases, and consumer electronics that make vast amounts of information available to users. The global information infrastructure encompasses a wide range of equipment, including cameras, scanners, keyboards, facsimile machines, computers, switches, compact disks, video and audio tape, cable, wire, satellites, fiber-optic transmission lines, networks of all types, televisions, monitors, printers, and much more. The friendly and adversary personnel who make decisions and handle the transmitted information constitute a critical component of the global information infrastructure. (JP 1-02)

High-payoff target

A target whose loss to the enemy will significantly contribute to the success of the friendly course of action. High-payoff targets are those high-value targets, identified through war-gaming, that must be acquired and successfully attacked for the success of the friendly commander’s mission. (JP 1-02)

High-value target

A target the enemy commander requires for the successful completion of the mission. The loss of high-value targets would be expected to seriously degrade important enemy functions throughout the friendly commander’s area of interest. (JP 1-02)

Human factors

In Information Operations, the psychological, cultural, behavioral, and other human attributes that influence decision-making, the flow of information, and the interpretation of information by individuals or groups at any level in a state or organization (JP 1-02)

Influence operations

(Air Force) Employment of capabilities to affect behaviors, protect operations, communicate commander’s intent, and project accurate information to achieve desired effects across the cognitive domain. These effects should result in differing behavior or a change in the adversary decision cycle, which aligns with the commander’s objectives (AFDD 2-5)

Information

1. Facts, data, or instructions in any medium or form. 2. The meaning that a human assigns to data by means of the known conventions used in their representation. (JP 1-02)

Information assurance (IA)

Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. Also called **IA.** (JP1-02)

Information environment

The aggregate of individuals, organizations or systems that collect, process, or disseminate information; also included is the information itself (JP 1-02)

Information management (IM)

The function of managing an organization’s information resources by the handling of knowledge acquired by one or many different individuals and organizations in a way that optimizes access by all who have a share in that knowledge or a right to that knowledge. (JP 1-02)

Information operations (IO)

The integrated employment of the core capabilities of Electronic Warfare (EW), Computer Network Operations (CNO), Psychological Operations (PSYOP), Military Deception (MILDEC), and Operations Security (OPSEC), in concert with specified supporting and related capabilities, to influence, disrupt, corrupt, or usurp adversarial human and automated decision-making while protecting our own. (D 3600.1/JP 3-13)

Information operations cell

(Army definition, but also functionally described within JP 3-13) A grouping of staff officers to plan, prepare and execute information operations formed around the information operations section. The output of the IO cell is input to the targeting cell. (FM 3-13)

IO capability specialist

A functional expert in one or more of the IO core capabilities (see IO Career Force, below next). They serve primarily in their specialty areas but may also serve as IO planners after receiving IO planner training. (D 3608.11)

IO career force

The military professionals that perform and integrate the core IO capabilities of EW, CNO, PSYOP, MILDEC, and OPSEC. The IO Career Force consists of IO Capability Specialists and IO Planners. (D 3608.11)

IO planner

A functional expert trained and qualified to execute full spectrum IO. They usually serve one or more tours as an IO capability specialist prior to assignment as an IO planner and may hold non-IO positions throughout their careers. (D 3608.11)

INFOCON

Information Operations Condition

Information security (INFOSEC)

The protection of information and information systems against unauthorized access or modification of information, whether in storage, processing, or transit, and against denial of service to authorized users. (JP 1-02)

Information superiority

The operational advantage derived from the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same. (JP 1-02)

Information systems (INFOSYS)

The entire infrastructure, organization, personnel, and components that collect, process, store, transmit, display, disseminate, and act on information. (JP 1-02)

Intelligence

1. The product resulting from the collection, processing, integration, analysis, evaluation, and interpretation of available information concerning foreign countries or areas. 2. Information and knowledge about an adversary obtained through observation, investigation, analysis, or understanding.

Interagency coordination

Within the context of Department of Defense involvement, the coordination that occurs between elements of Department of Defense, and engaged US Government agencies, nongovernmental organizations, and regional and international organizations for the purpose of accomplishing an objective. [JP 1-02]

Joint intelligence preparation
of the battlespace (JIPB)

The analytical process used by joint intelligence organizations to produce intelligence assessments, estimates, and other intelligence products in support of the joint force commander's decision-making process. It is a continuous process that includes defining the total battlespace environment; describing the battlespace's effects; evaluating the adversary; and determining and describing adversary potential courses of action. The process is used to analyze the air, land, sea, space, electromagnetic, cyberspace, and human dimensions of the environment and to determine an opponent's capabilities to operate in each. Joint intelligence preparation of the battlespace products are used by the joint force and component command staffs in preparing their estimates and are also applied during the analysis and selection of friendly courses of action. (JP 1-02)

Joint restricted frequency list (JRFL)

A time and geographically-oriented listing of TABOO, PROTECTED, and GUARDED functions, nets, and frequencies. It should be limited to the minimum number of frequencies necessary for friendly forces to accomplish objectives. **TABOO frequencies -** Any friendly frequency of such importance that it must never be deliberately jammed or interfered with by friendly forces. Normally, these frequencies include international distress, CEASE BUZZER, safety, and controller frequencies. These frequencies are generally long standing. However, they may be time-oriented in that, as the combat or exercise situation changes, the restrictions may be removed. (JP 1-02)

Joint targeting coordination board (JTCB)

A group formed by the joint force commander to accomplish broad targeting oversight functions that may include but are not limited to coordinating targeting information, providing targeting guidance and priorities, and refining the joint integrated prioritized target list. The board is normally comprised of representatives from the joint force staff, all components and, if required, component subordinate units. (JP 1-02)

Measure of effectiveness (MOE)

A criterion used to assess changes in system behavior, capability, or operational environment that is tied to measuring the attainment of an end state, achievement of an objective, or creation of an effect.. (JP 1-02)

Military deception (MILDEC)

Actions executed to deliberately mislead adversary military decision makers as to friendly military capabilities, intentions, and operations, thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly mission. (JP 1-02)

Network-centric warfare

An information superiority-enabled concept of operations that generates increased combat power by networking sensors, decision makers, and shooters to achieve shared awareness, increased speed of command, higher tempo of operations, greater lethality, increased survivability, and a degree of self-synchronization. (Network Centric Warfare: CCRP Publication)

Nongovernmental organization (NGO)

A private, self-governing, not-for-profit organization dedicated to alleviating human suffering; and/or promoting education, health care, economic development, environmental protection, human rights, and conflict resolution; and/or encouraging the establishment of democratic institutions and civil society. (JP 1-02)

Operations security (OPSEC)

A process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to: a. identify those actions that can be observed by adversary intelligence systems; b. determine indicators that adversary intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries; and c. select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation. (JP 1-02)

Perception management

(Army) Actions to convey and/or deny selected information and indicators to foreign audiences to influence their emotions, motives, and objective reasoning as well as to intelligence systems and leaders at all levels to influence official estimates, ultimately resulting in foreign behaviors and official actions favorable to the originator's objectives. In various ways, perception management combines truth projection, operations security, cover and deception, and psychological operations. (FM 3-13)

Physical destruction

(Army) The application of combat power to destroy or neutralize adversary forces and installations. It includes direct and indirect forces from ground, sea, and air forces. Also included are direct actions by special operations forces. (FM 3-13)

Physical security

1. That part of security concerned with physical measures designed to safeguard personnel; to prevent unauthorized access to equipment,

installations, material, and documents; and to safeguard them against espionage, sabotage, damage, and theft. 2. **(only)** In communications security, the component that results from all physical measures necessary to safeguard classified equipment, material, and documents from access thereto or observation thereof by unauthorized persons. See also communications security; security. (JP1-02)

Priority national intelligence objectives

A guide for the coordination of intelligence collection and production in Response to requirements relating to the formulation and execution of national security policy. They are compiled annually by the Washington Intelligence Community and flow directly from the intelligence mission as set forth by the National Security Council. They are specific enough to provide a basis for planning the allocation of collection and research resources, but not so specific as to constitute in themselves research and collection requirements. (JP 1-02)

Propaganda

Any form of communication in support of national objectives designed to influence the opinions, emotions, attitudes, or behavior of any group in order to benefit the sponsor, either directly or indirectly. See also black propaganda; grey propaganda; white propaganda. (JP 1-02)

Psychological operations (PSYOP)

Planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals. The purpose of psychological operations is to induce or reinforce foreign attitudes and behavior favorable to the originator's objectives. (JP1-02)

Psychological operations assessment team (POAT)

A small, tailored team (approximately 4-12 personnel) that consists of psychological operations planners and product distribution/ dissemination and logistic specialists. The team is deployed to theater at the request of the combatant commander to assess the situation, develop psychological operations objectives, and recommend the appropriate level of support to accomplish the mission. (JP 1-02)

Psychological operations Impact indicators

An observable event or a discernible subjectively determined behavioral change that represents an effect of a psychological operations activity on the intended foreign target audience at a particular point in time. It is measured evidence, ascertained during the analytical phase of the psychological operations development process, to evaluate the degree to which the psychological operations objective is achieved. (JP 1-02)

Psychological operations support element (JPSE)

A tailored element that can provide limited psychological operations support. Psychological operations support elements do not contain organic command and control capability; therefore, command relationships must be clearly defined. The size, composition and capability of the psychological operations support element are determined by the requirements of the supported commander. A psychological operations support element is not designed to provide full-spectrum psychological operations capability; reach-back is critical for its mission success. (JP 1-02)

Public affairs (PA)

Those public information, command information, and community relations activities directed toward both the external and internal public with interest in the DoD. (JP 1-02)

Public diplomacy (PD)

Those overt international public information activities of the United States Government designed to promote United States foreign policy objectives by seeking to understand, inform, and influence foreign audiences and opinion makers, and by broadening the dialogue between American citizens and institutions and their counterparts abroad. (JP 1-02)

Public information

Information of a military nature, the dissemination of which through public news media is not inconsistent with security, and the release of which is considered desirable or non-objectionable to the responsible releasing agency. (JP 1-02)

Reachback
The process of obtaining products, services, and applications, or forces, or equipment, or material from organizations that are not forward deployed. (JP 1-02)

Strategic communication
Focused United States Government (USG) efforts to understand and engage key audiences in order to create, strengthen or preserve conditions favorable for the advancement of USG interests, policies, and objectives through the use of coordinated programs, plans, themes, messages, and products synchronized with the actions of all elements of national power. (JP 1-02)

Target audience (TA)
An individual or group selected for influence. (JP 1-02.)

The Dictionary of Military and Associated Terms is available on line at:
http://www.dtic.mil/doctrine/jpreferencepubs.htm

Last updated: November 2009